EXHIBIT C

HPE Aruba Claim Chart

U.S. Patent 10,592,275

System and method for swarm collaborative intelligence using dynamically configurable proactive co-processing cells

References

[Reference 1] Aruba GreenLake platform
[Reference 2] Aruba Central Is Now Part of HPE GreenLake
[Reference 3] About Aruba Central
[Reference 4] Accessing the Aruba Central Portal
[Reference 5] HPE GreenLake for Device Management
[Reference 6] About the Aruba Central App User Interface
[Reference 7] Device Configuration Methods in Aruba Central
[Reference 8] Configuring Access Points in HPE Aruba Networking Central
[Reference 9] Automatic Retrieval of Configuration
[Reference 10] How do devices communicate with HPE Aruba Networking Central?
[Reference 11] Automatic Rollback Configuration
[Reference 12] Viewing Configuration Status
[Reference 13] Managing Sites
[Reference 14] Example Use Case
[Reference 15] VXLAN Interoperability | ArubaOS-Switch Configuration Guide

HPE Aruba Supported Devices

500 Series Campus Access Points
550 Series Campus Access Points
530 Series Campus Access Points
510 Series Campus Access Points
670 and 670EX Series Outdoor Access Points
600H Series Hospitality Access Point
600R Series and 500R Series Remote Access Points

Patent '275 Claim Elements	HPE Aruba
1. A collaborative intelligence system, comprising:	"HPE GreenLake orchestrates and manages network, compute, storage, and supporting services. It unifies security, visibility, and management in a scalable, cloud-native solution. AI-powered insights, workflow automation, and edge-to-cloud security provide a single source control across campus, data center, branch, and IoT networks." [Reference 1, Aruba GreenLake Platform] "Aruba Central Is Now Part of HPE GreenLake" [Reference 2, Aruba Central Is Now Part of HPE GreenLake] "Aruba Central is a powerful cloud networking solution that offers simplicity for today's networks. As the management and orchestration console for Aruba ESP (Edge Services Platform)" [Reference 3, About Aruba Central]
a task pool;	"Aruba Central is a powerful cloud networking solution that offers simplicity for today's networks. As the management and orchestration console for Aruba ESP (Edge Services Platform)" [Reference 3, About Aruba Central] Also, see Figure 1.

	"If you are accessing the login URL from the www.arubanetworks.com website, ensure that you select the zone in which your account was created." [Reference 4, Accessing Aruba Central Portal] "**Logging in to Aruba Central** To log in to Aruba Central: 1. Access the Aruba Central login URL for your zone. 2. Notice that the zone is automatically selected based on your geographical location. 3. Enter the email address and click Continue. 4. Log in using your credentials." [Reference 4, Accessing Aruba Central Portal] "With the HPE GreenLake for Device Management API, you can view, manage, and onboard devices in your workspace. The API allows you to initiate any operation or task that is available through the HPE GreenLake edge-to-cloud platform UI." [Reference 5, HPE GreenLake for Device Management]
a controller configured to populate the task pool with a plurality of first tasks and a plurality of second tasks;	"**Navigating to the Switch, Access Point, or Gateway Dashboard** In the Aruba Central app, you can navigate to a device dashboard for a switch, access point, or gateway. The device dashboard enables you to monitor, troubleshoot, or configure a single device. . . . **Workflow to Configure, Monitor, or Troubleshoot in the Aruba Central app** The following image [see Figure 2] displays a flowchart to help you navigate the Aruba Central app to complete any task." [Reference 6, About the Aruba Central App User Interface] "**Device Configuration Methods in Aruba Central** Aruba Central offers the following options for configuring devices in your account: **Groups**—You can use the Groups feature to create a logical subset of devices. If you have devices that must share common configuration settings, ensure that you assign these devices to the same group. Any new device joining a group inherits the configuration that is already applied on the devices in a group. **Device-specific configuration**—If you have fewer devices that do not have the same configuration requirements, you can apply configuration changes at the device level. In some cases, although the devices are assigned to a group, you may want to have a slightly different configuration on one specific device in a group. In such cases, you can modify the device configuration and apply changes at the device level" [Reference 7, Device Configuration Methods in Aruba Central]
a first co-processor configured to successively: proactively retrieve a first task from the task pool;	"HPE Aruba Networking Central allows you to configure various AP properties such as WLAN SSID profiles, radio profiles, authentication and security parameters, along with system parameters in both Instant APs and HPE Aruba Networking Wireless Operating System 10 APs." [Reference 8, Configuring Access Points in HPE Aruba Networking Central] "Instant APs support managed mode operations to retrieve the configuration file from a server through the FTP or FTPS, and automatically update the Instant AP configuration. The server details for retrieving configuration files are stored in the basic configuration of the Instant APs. The basic configuration of an Instant AP includes settings specific to an Instant AP, for example, host name, static IP, and radio configuration settings. When an Instant AP boots up, it performs a GET operation to retrieve the configuration (.cfg) file from the associated server using the specified download method. After the initial configuration is applied to the Instant APs, the configuration can be changed at any point. You can configure a polling mechanism to fetch the latest configuration by using an FTP or FTPS client periodically. If the remote configuration

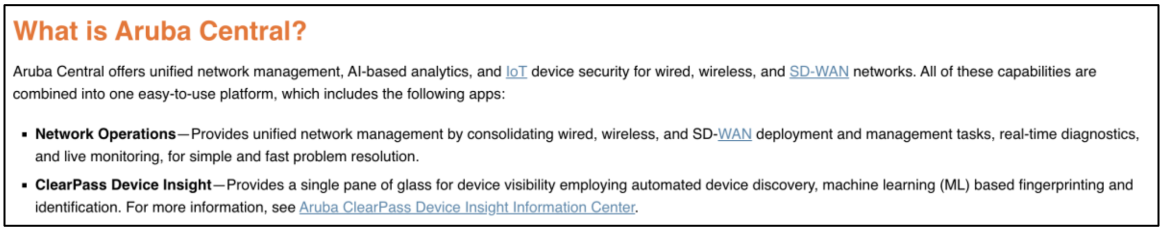
	is different from the one running on the Instant AP and if a difference in the configuration file is detected by the Instant AP, the new configuration is applied. At any given time, Instant APs can fetch only one configuration file, which may include the configuration details specific to an Instant AP." [Reference 9, Automatic Retrieval of Configuration] "If HPE Aruba Networking Central is set as the management entity, devices automatically connect to HPE Aruba Networking Central." [Reference 10, How do devices communicate with HPE Aruba Networking Central?] "The auto-rollback mechanism is triggered when the switch loses connectivity to Aruba Central after the configuration is applied. The switch rolls back to the last known stable configuration and reconnects to Aruba Central." [Reference 11, Automatic Rollback Configuration]
process the first task;	"If the remote configuration is different from the one running on the Instant AP and if a difference in the configuration file is detected by the Instant AP, the new configuration is applied." [Reference 9, Automatic Retrieval of Configuration]
generate first resulting data;	"Viewing Configuration Status Aruba Central provides an audit dashboard for reviewing configuration changes for the devices provisioned in UI and template groups. The Configuration Audit page is available for Instant APs, switches, and gateways." [Reference 12, Viewing Configuration Status]
and update the task pool to reflect completion of the first task, all without any communication between the first co-processor and the controller;	"Viewing Configuration Status Aruba Central provides an audit dashboard for reviewing configuration changes for the devices provisioned in UI and template groups. The Configuration Audit page is available for Instant APs, switches, and gateways." [Reference 12, Viewing Configuration Status] "The Configuration Sync Issues window is displayed with the following tabs: **Not In Sync Configuration**—Displays the configuration changes that are not synched with the switch. **Device Running Configuration**—Displays the running configuration on the switch." [Reference 12, Viewing Configuration Status] Device configuration completes **without communication** with the app (controller), in fact, the app needs to connect to Aruba Central to view the configuration change: "To view the Configuration Audit page, complete the following steps: For Instant APs: In the Aruba Central app, set the filter to a group that contains at least one AP. . . . The Configuration Audit details page is displayed. For Aruba switches: In the Aruba Central app, set the filter to a group that contains at least one switch. . . . The Configuration Audit details page is displayed. For Aruba gateways: In the Aruba Central app, set the filter to a group that contains at least one Branch . . . The tabs to configure gateways are displayed." [Reference 12, Viewing Configuration Status]

and a second co-processor configured to successively: proactively retrieve a second task from the task pool;	"HPE Aruba Networking Central allows you to configure various AP properties such as WLAN SSID profiles, radio profiles, authentication and security parameters, along with system parameters in both Instant APs and HPE Aruba Networking Wireless Operating System 10 APs." [Reference 8, Configuring Access Points in HPE Aruba Networking Central] "Instant APs support managed mode operations to retrieve the configuration file from a server through the FTP or FTPS, and automatically update the Instant AP configuration. The server details for retrieving configuration files are stored in the basic configuration of the Instant APs. The basic configuration of an Instant AP includes settings specific to an Instant AP, for example, host name, static IP, and radio configuration settings. When an Instant AP boots up, it performs a GET operation to retrieve the configuration (.cfg) file from the associated server using the specified download method. After the initial configuration is applied to the Instant APs, the configuration can be changed at any point. You can configure a polling mechanism to fetch the latest configuration by using an FTP or FTPS client periodically. If the remote configuration is different from the one running on the Instant AP and if a difference in the configuration file is detected by the Instant AP, the new configuration is applied. At any given time, Instant APs can fetch only one configuration file, which may include the configuration details specific to an Instant AP." [Reference 9, Automatic Retrieval of Configuration] "If HPE Aruba Networking Central is set as the management entity, devices automatically connect to HPE Aruba Networking Central." [Reference 10, How do devices communicate with HPE Aruba Networking Central?] "The auto-rollback mechanism is triggered when the switch loses connectivity to Aruba Central after the configuration is applied. The switch rolls back to the last known stable configuration and reconnects to Aruba Central." [Reference 11, Automatic Rollback Configuration]
process the second task;	"If the remote configuration is different from the one running on the Instant AP and if a difference in the configuration file is detected by the Instant AP, the new configuration is applied." [Reference 9, Automatic Retrieval of Configuration]
generate second resulting data;	"Viewing Configuration Status Aruba Central provides an audit dashboard for reviewing configuration changes for the devices provisioned in UI and template groups. The Configuration Audit page is available for Instant APs, switches, and gateways." [Reference 12, Viewing Configuration Status]
and update the task pool to reflect completion of the second task, all without any communication between the second co-processor and the controller;	"Viewing Configuration Status Aruba Central provides an audit dashboard for reviewing configuration changes for the devices provisioned in UI and template groups. The Configuration Audit page is available for Instant APs, switches, and gateways." [Reference 12, Viewing Configuration Status] "The Configuration Sync Issues window is displayed with the following tabs: **Not In Sync Configuration**—Displays the configuration changes that are not synched with the switch. **Device Running Configuration**—Displays the running configuration on the switch." [Reference 12, Viewing Configuration Status] Device configuration completes **without communication** with the app (controller), in fact, the app needs to connect to Aruba Central to view the configuration change:

	"To view the Configuration Audit page, complete the following steps: For Instant APs: In the Aruba Central app, set the filter to a group that contains at least one AP. . . . The Configuration Audit details page is displayed. For Aruba switches: In the Aruba Central app, set the filter to a group that contains at least one switch. . . . The Configuration Audit details page is displayed. For Aruba gateways: In the Aruba Central app, set the filter to a group that contains at least one Branch . . . The tabs to configure gateways are displayed." [Reference 12, Viewing Configuration Status]
wherein the collaborative intelligence system is configured to dynamically accept the first co-processor, the second co-processor, and an additional co-processor into the processing system on a plug-and-play basis without any communication with the controller;	"HPE GreenLake orchestrates and manages network, compute, storage, and supporting services. It unifies security, visibility, and management in a scalable, cloud-native solution. AI-powered insights, workflow automation, and edge-to-cloud security provide a single source control across campus, data center, branch, and IoT networks." [Reference 1, Aruba GreenLake Platform] "If HPE Aruba Networking Central is set as the management entity, devices automatically connect to HPE Aruba Networking Central." [Reference 10, How do devices communicate with HPE Aruba Networking Central?] Device configuration completes **without communication** with the app (controller), in fact, the app needs to connect to Aruba Central to view the configuration change: "To view the Configuration Audit page, complete the following steps: For Instant APs: In the Aruba Central app, set the filter to a group that contains at least one AP. . . . The Configuration Audit details page is displayed. For Aruba switches: In the Aruba Central app, set the filter to a group that contains at least one switch. . . . The Configuration Audit details page is displayed. For Aruba gateways: In the Aruba Central app, set the filter to a group that contains at least one Branch . . . The tabs to configure gateways are displayed." [Reference 12, Viewing Configuration Status]
the plurality of first tasks and the plurality of second tasks are associated with a common objective;	"Aruba Central allows you to configure multiple devices in bulk using templates. However, in some cases, the configuration parameters may vary per device. To address this, Aruba Central identifies some customizable CLI parameters as variables and allows you to modify the definitions for these variables as per your requirements." [Reference 13, Managing Sites] "Sites are used to group devices by a physical location. You can assign devices to a site to group them and monitor based on the site name." [Reference 13, Managing Sites]

the first and second co-processors autonomously work together in solidarity with the task pool to complete the common objective.	"Instant APs support managed mode operations to retrieve the configuration file from a server through the FTP or FTPS, and automatically update the Instant AP configuration." [Reference 9, Automatic Retrieval of Configuration] "In the use case, the goal is to enable role-based micro-segmentation across all wired and wireless clients in an enterprise campus. Roles and role-based policies are orchestrated centrally from the Client Roles page on Aruba Central. These policies are enforced on the edge VTEPs in a distributed EVPN fabric for wired clients and on the WLAN gateways for wireless clients. The VXLAN-EVPN fabric is provisioned on the AOS-CX switches using the Fabric Provisioning Wizard on Aruba Central. As depicted in the above diagram, wired and wireless clients that are assigned the employee role are allowed to communicate with other clients with the Employee role, but not to the clients with the IoT role. Conversely, clients with the IoT role are denied access to clients of both the IoT and employee role." [Reference 14, Example Use Case] "Aruba 3810M Switch Series as VTEP" [Reference 15, VXLAN Interoperability | ArubaOS-Switch Configuration Guide]

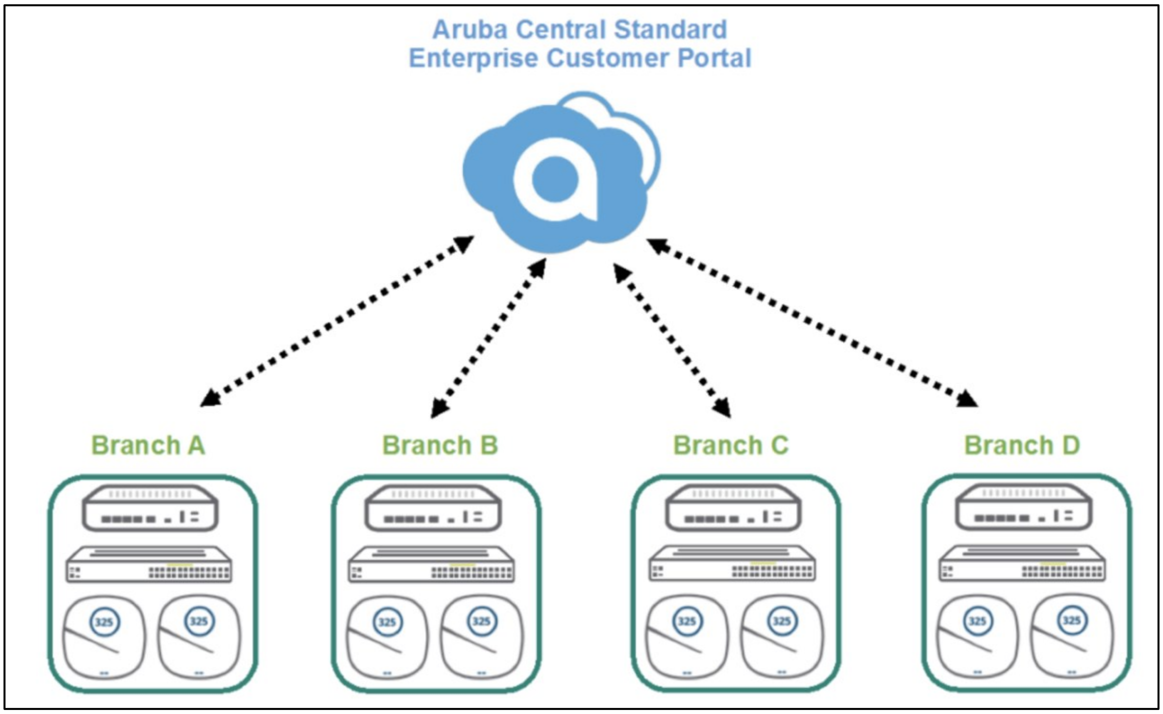
FIG. 1



What is Aruba Central?

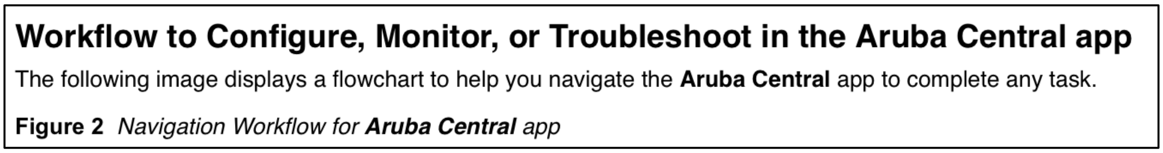
Aruba Central offers unified network management, AI-based analytics, and IoT device security for wired, wireless, and SD-WAN networks. All of these capabilities are combined into one easy-to-use platform, which includes the following apps:

- **Network Operations**—Provides unified network management by consolidating wired, wireless, and SD-WAN deployment and management tasks, real-time diagnostics, and live monitoring, for simple and fast problem resolution.
- **ClearPass Device Insight**—Provides a single pane of glass for device visibility employing automated device discovery, machine learning (ML) based fingerprinting and identification. For more information, see Aruba ClearPass Device Insight Information Center.



https://www.arubanetworks.com/techdocs/central/2.5.2/content/nms/overview/overview.htm

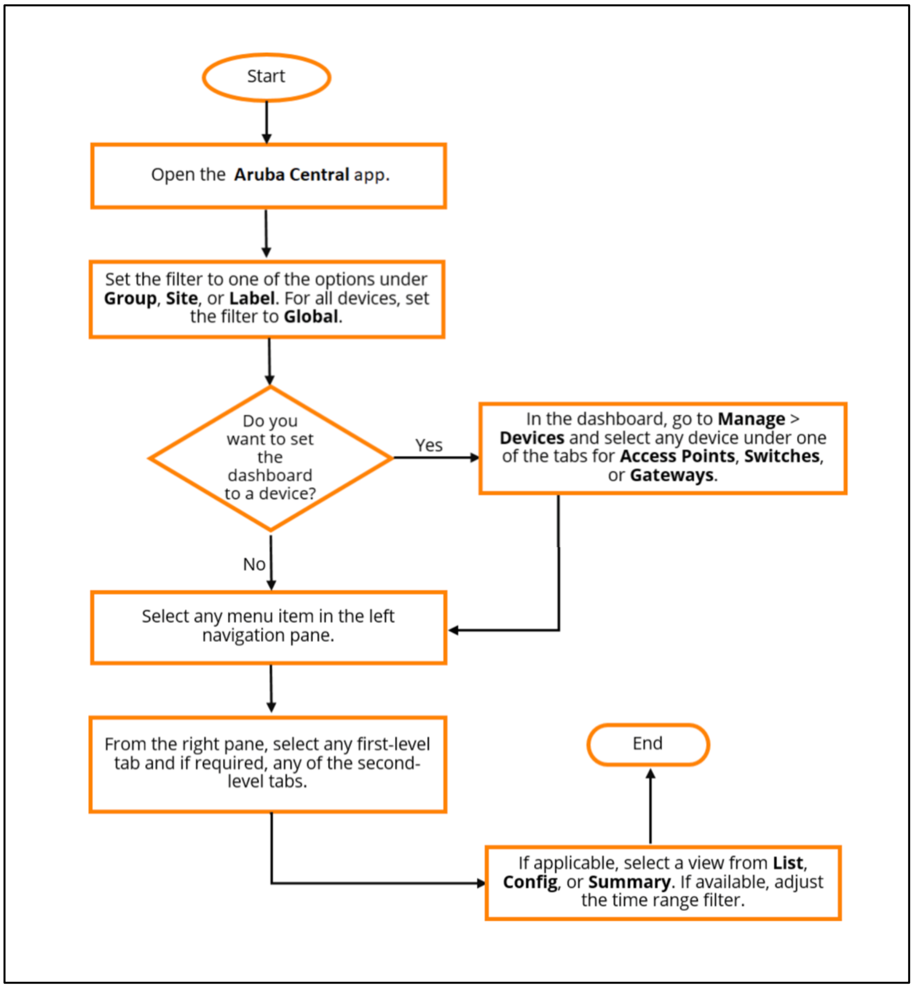
FIG. 2



Workflow to Configure, Monitor, or Troubleshoot in the Aruba Central app

The following image displays a flowchart to help you navigate the **Aruba Central** app to complete any task.

Figure 2 *Navigation Workflow for **Aruba Central** app*


Start
Open the **Aruba Central** app.
Set the filter to one of the options under **Group**, **Site**, or **Label**. For all devices, set the filter to **Global**.
Do you want to set the dashboard to a device?
Yes
In the dashboard, go to **Manage** > **Devices** and select any device under one of the tabs for **Access Points**, **Switches**, or **Gateways**.
No
Select any menu item in the left navigation pane.
From the right pane, select any first-level tab and if required, any of the second-level tabs.
If applicable, select a view from **List**, **Config**, or **Summary**. If available, adjust the time range filter.
End

https://www.arubanetworks.com/techdocs/central/2.5.5/content/nms/overview/user_interface.htm

REFERENCE 1

Hewlett Packard Enterprise

Edge Services Platform / GreenLake Platform

28-Mar-24

GreenLake Platform

The HPE GreenLake platform is a portfolio of cloud and as-a-service solutions tailored to address complex network management needs effectively and efficiently.

HPE GreenLake orchestrates and manages network, compute, storage, and supporting services. It unifies security, visibility, and management in a scalable, cloud-native solution. AI-powered insights, workflow automation, and edge-to-cloud security provide a single source control across campus, data center, branch, and IoT networks.

Network devices managed by Aruba Central are maintained and licensed in HPE GreenLake's inventory. This chapter describes setting up HPE GreenLake, provisioning devices, and attaching licenses to devices.

▼ Table of contents

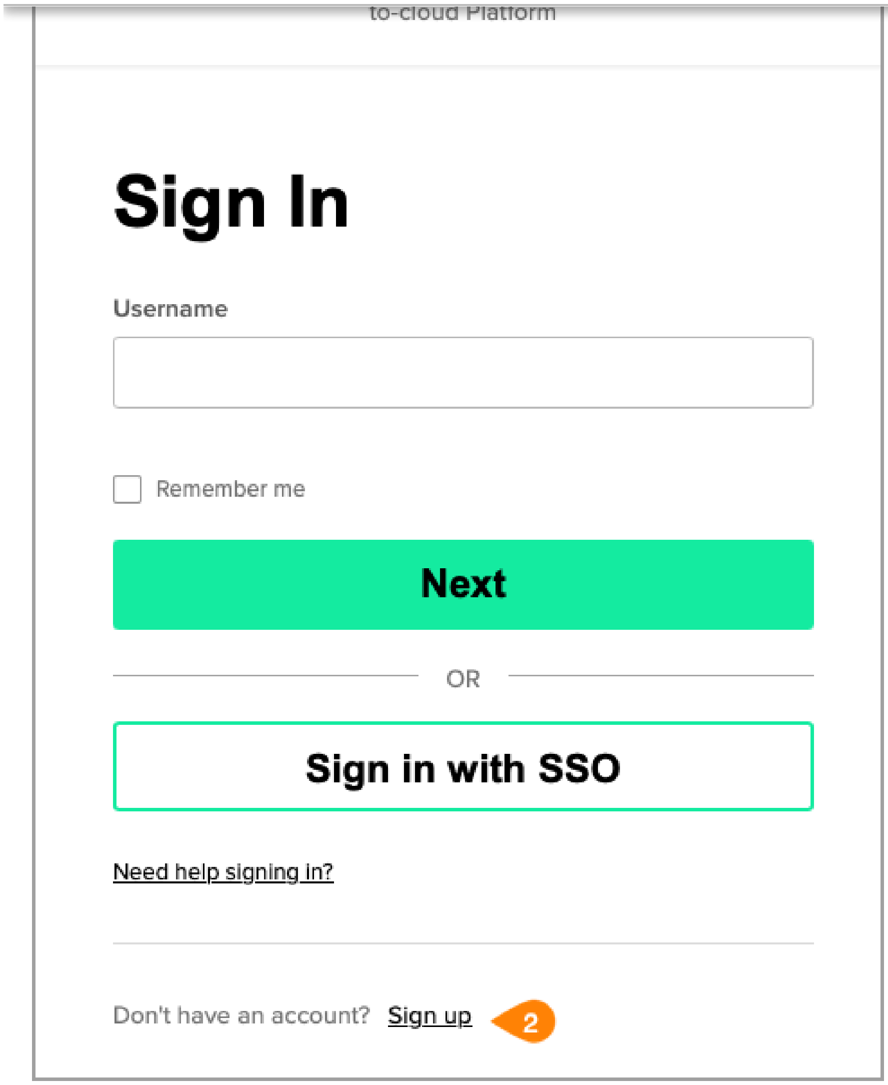
Feedback

Create a HPE GreenLake Account

The following procedure creates a HPE GreenLake Account.

Step 1 Navigate to the **HPE GreenLake** homepage.

Step 2 Click **Sign up**.



to-cloud Platform

Sign In

Username

□ Remember me

Next

OR

Sign in with SSO

Need help signing in?

Don't have an account? Sign up

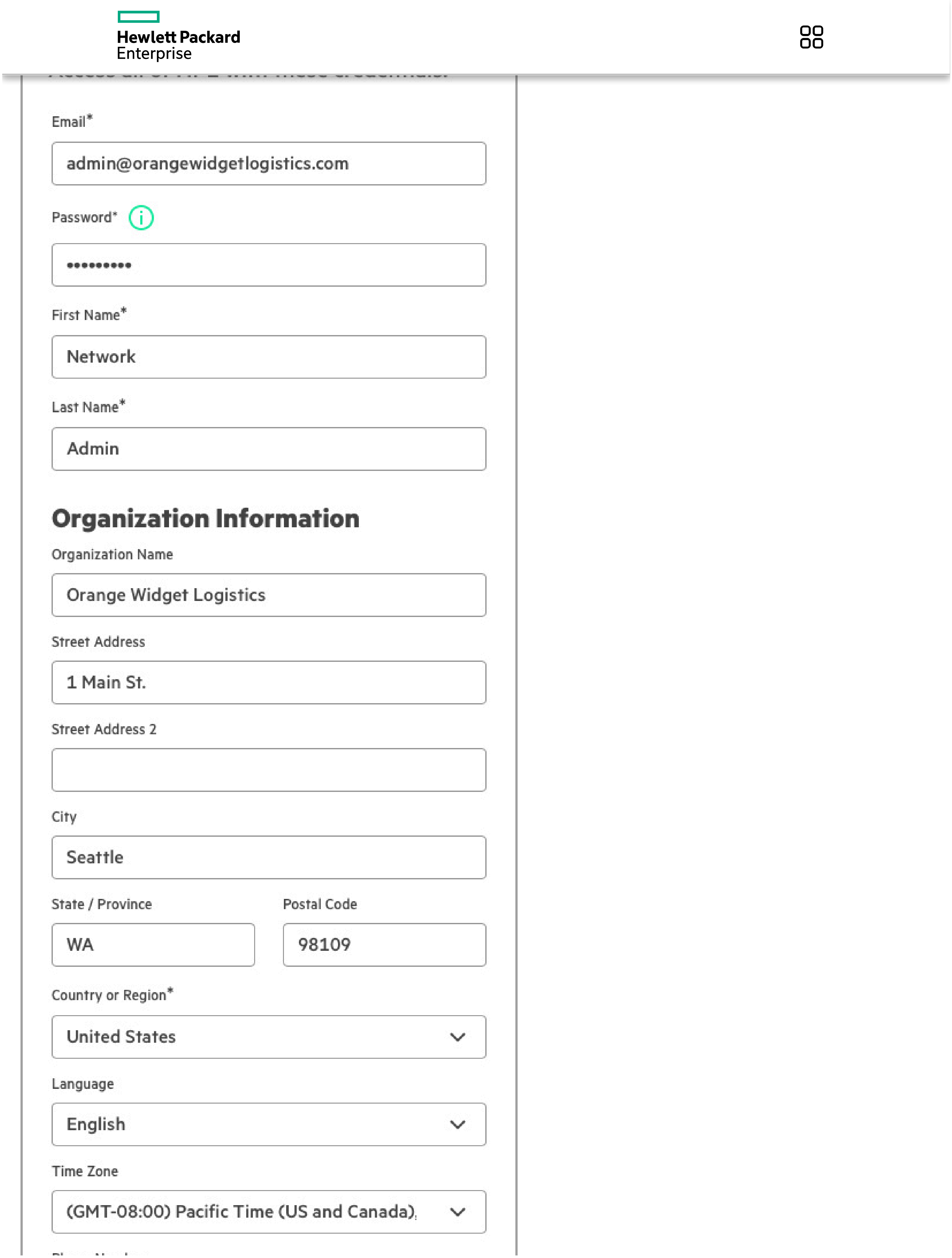
Step 3 Complete the fields and click **Create Account**.

The following example values are used to create an account for network administrator at Orange Widget Logistics:

- **Email:** *admin@orangewidgetlogistics.com*
- **Password:** *password*
- **First Name:** *Network*
- **Last Name:** *Admin*
- **Organization Name:** *Orange Widget Logistics*
- **Street Address:** *1 Main St.*
- **City:** *Seattle*
- **State:** *WA*
- **Postal Code:** *98109*
- **Country:** *United States*

- **Phone Number:** *+1 206 111 1111*

[Reference 1]



Hewlett Packard Enterprise

Email*

admin@orangewidgetlogistics.com

Password*

••••••••••

First Name*

Network

Last Name*

Admin

Organization Information

Organization Name

Orange Widget Logistics

Street Address

1 Main St.

Street Address 2

City

Seattle

State / Province

WA

Postal Code

98109

Country or Region*

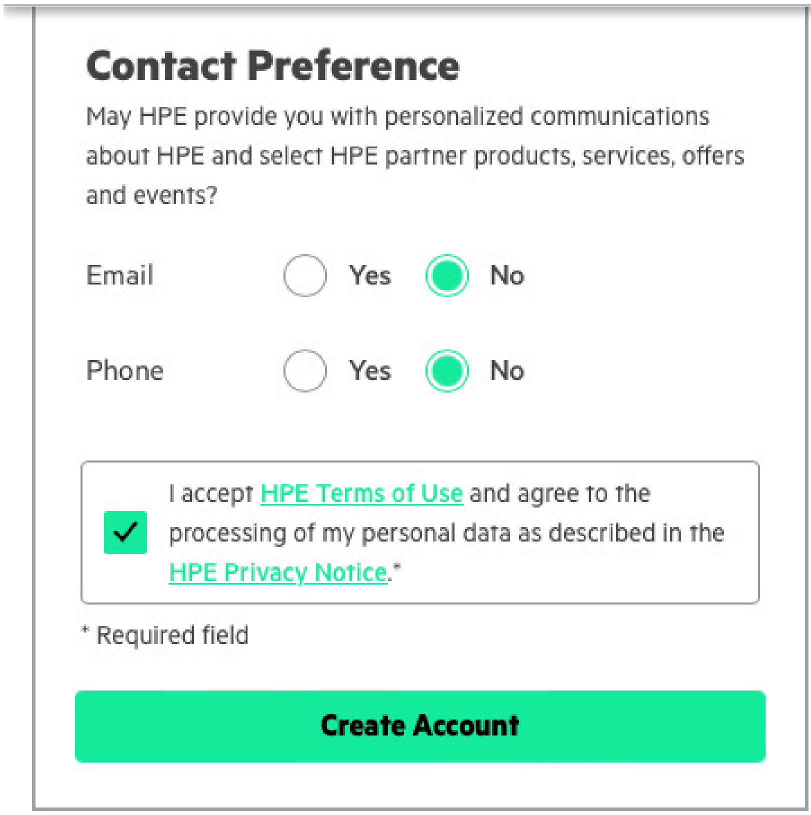
United States

Language

English

Time Zone

(GMT-08:00) Pacific Time (US and Canada),



Contact Preference

May HPE provide you with personalized communications about HPE and select HPE partner products, services, offers and events?

Email ○ Yes ● No

Phone ○ Yes ● No

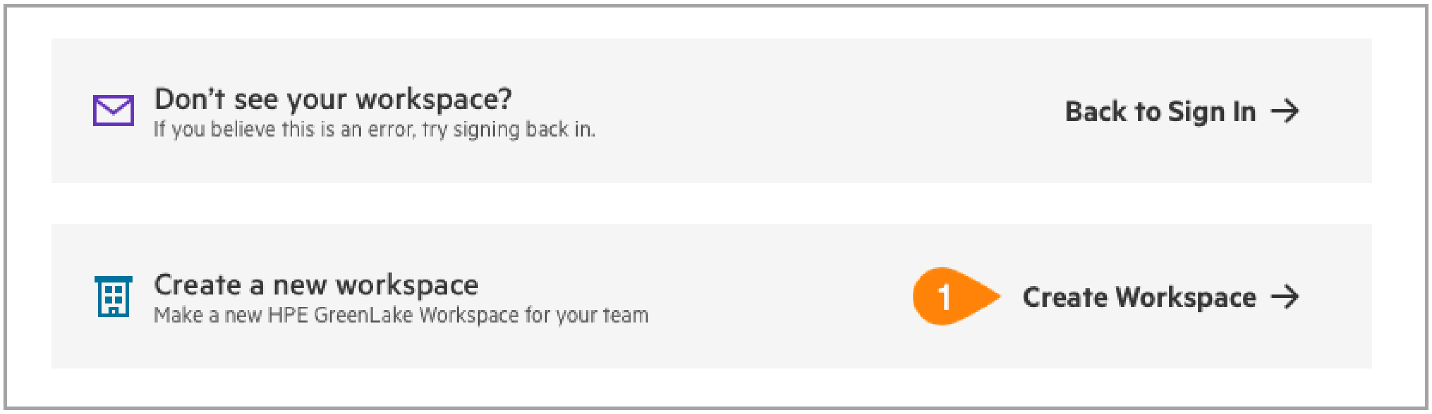
☑ I accept HPE Terms of Use and agree to the processing of my personal data as described in the HPE Privacy Notice.*

* Required field

Create a Company Workspace

The following procedure creates a company workspace to manage a set of HPE products, applications, and services for a single company. Users can create additional workspaces as needed to provide secure, segregated access to distinct groups of resources.

Step 1 Login to the GreenLake account and select **Create Workspace**.



Don’t see your workspace?
If you believe this is an error, try signing back in.

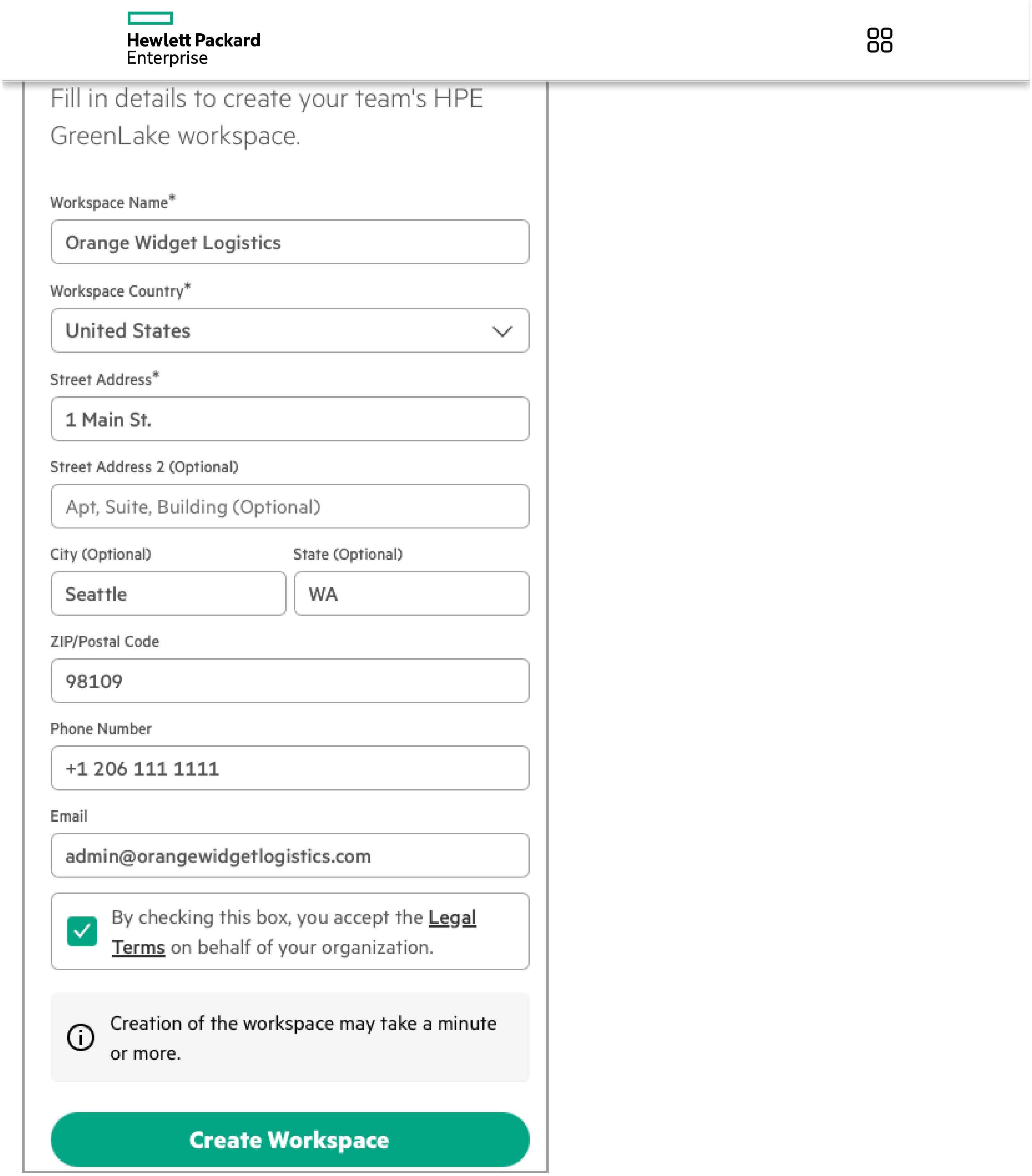
Create a new workspace
Make a new HPE GreenLake Workspace for your team

Step 2 Enter the details and click **Create Workspace**.

The following sample values are used to create a workspace for Orange Widget Logistics:

- **Workspace Name:** *Orange Widget Logistics*
- **Workspace Country:** *United States*

- **State:** *WA*
- **Postal Code:** *98109*
- **Phone Number:** *+1 206 111 1111*
- **Email:** *admin@orangewidgetlogistics.com*



Fill in details to create your team's HPE GreenLake workspace.

Workspace Name*
Orange Widget Logistics

Workspace Country*
United States

Street Address*
1 Main St.

Street Address 2 (Optional)
Apt, Suite, Building (Optional)

City (Optional)
Seattle

State (Optional)
WA

ZIP/Postal Code
98109

Phone Number
+1 206 111 1111

Email
admin@orangewidgetlogistics.com

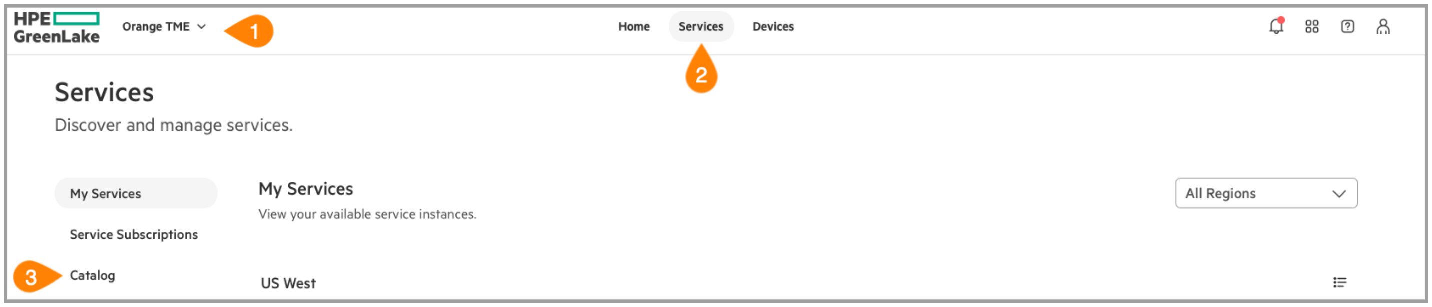
☑ By checking this box, you accept the Legal Terms on behalf of your organization.

Creation of the workspace may take a minute or more.

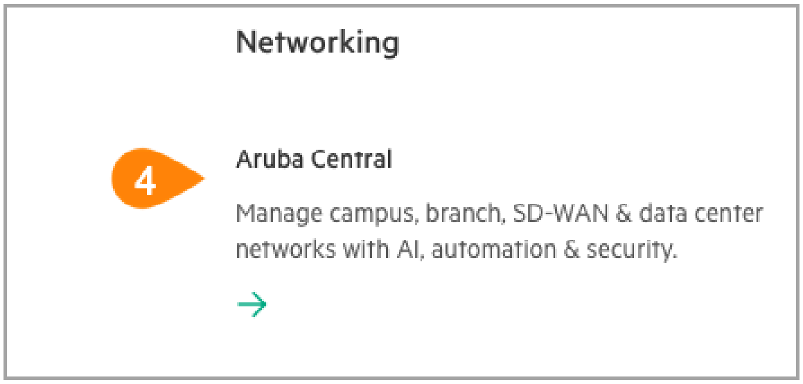
Add Aruba Central to the GreenLake Workspace

The following procedure adds the Aruba Central cloud application to the HPE GreenLake workspace.

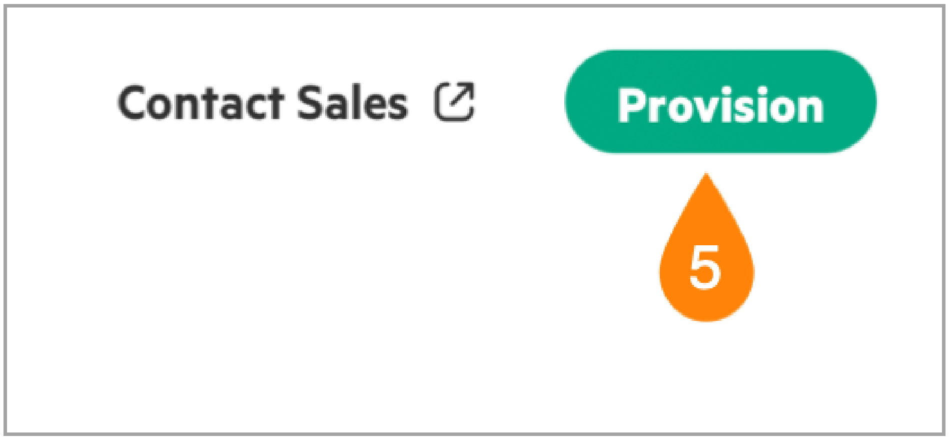
Step 1 Login to GreenLake and select the appropriate Workspace.



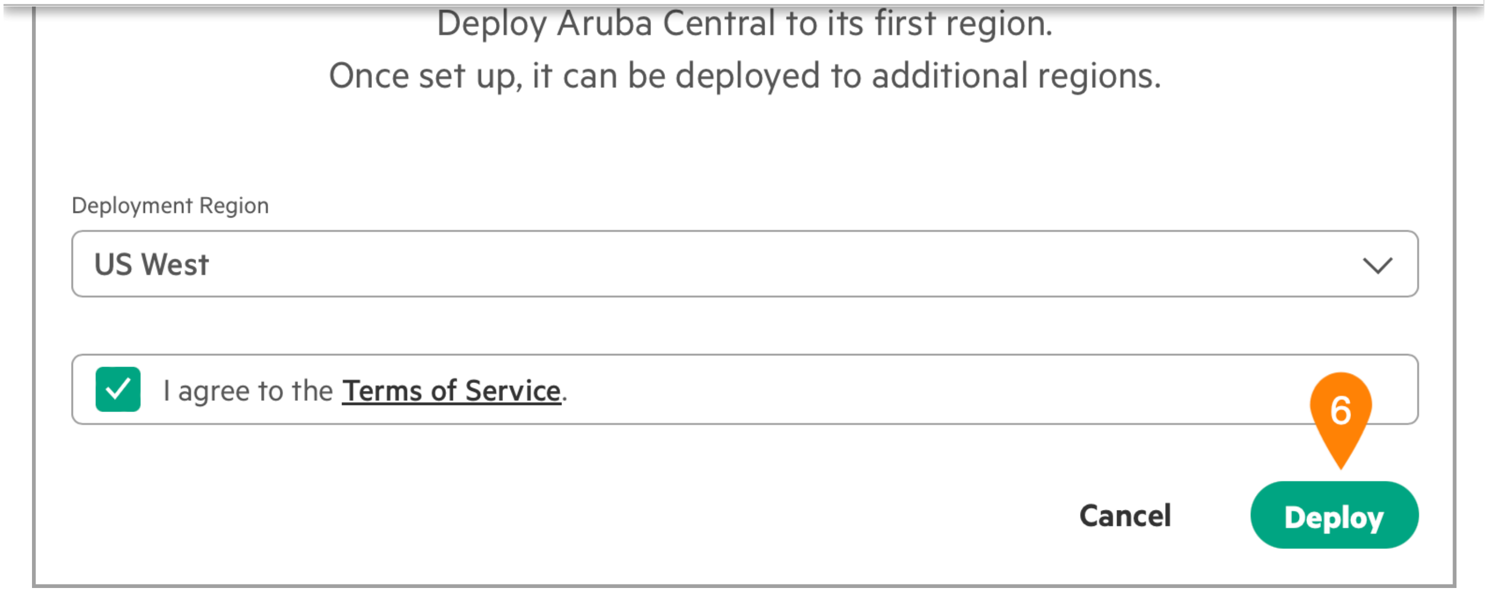
Step 4 Select **Aruba Central** in Networking section.


Networking
4
Aruba Central
Manage campus, branch, SD-WAN & data center networks with AI, automation & security.

Step 5 Click **Provision**.



Step 6 Select an appropriate **Deployment Region**, check the checkbox beside **I agree to the Terms of Service**, and click **Deploy**.

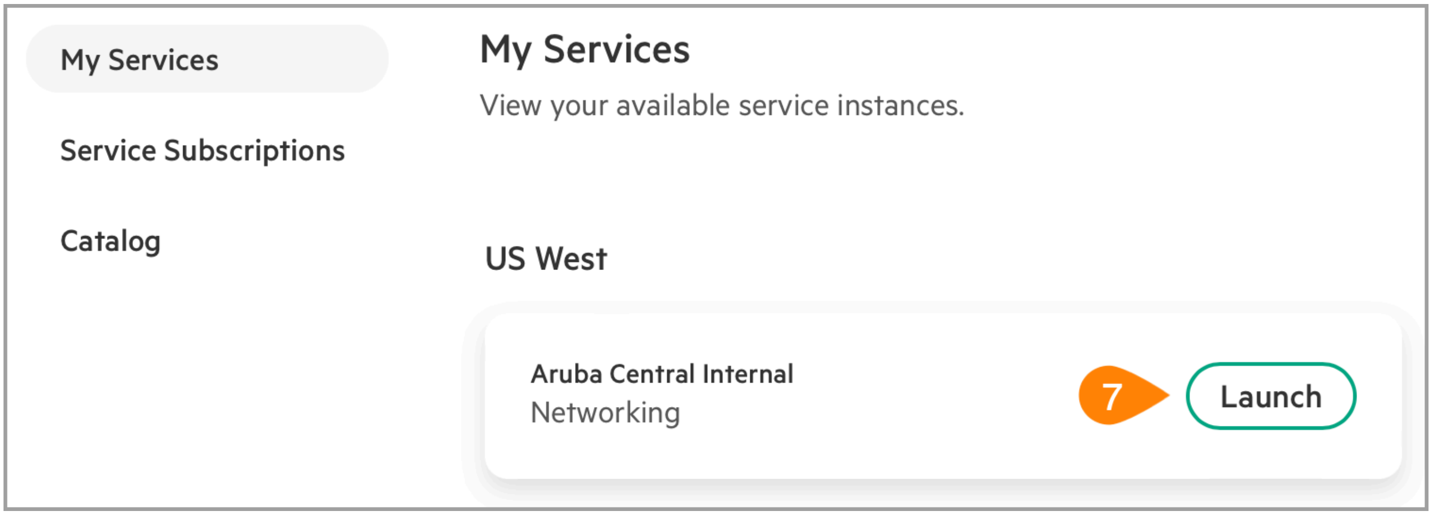


Deploy Aruba Central to its first region.
Once set up, it can be deployed to additional regions.

Deployment Region: US West

☑ I agree to the Terms of Service.

Step 7 Click **My Services** on the left menu, then click **Launch** in the Aruba Central tile.

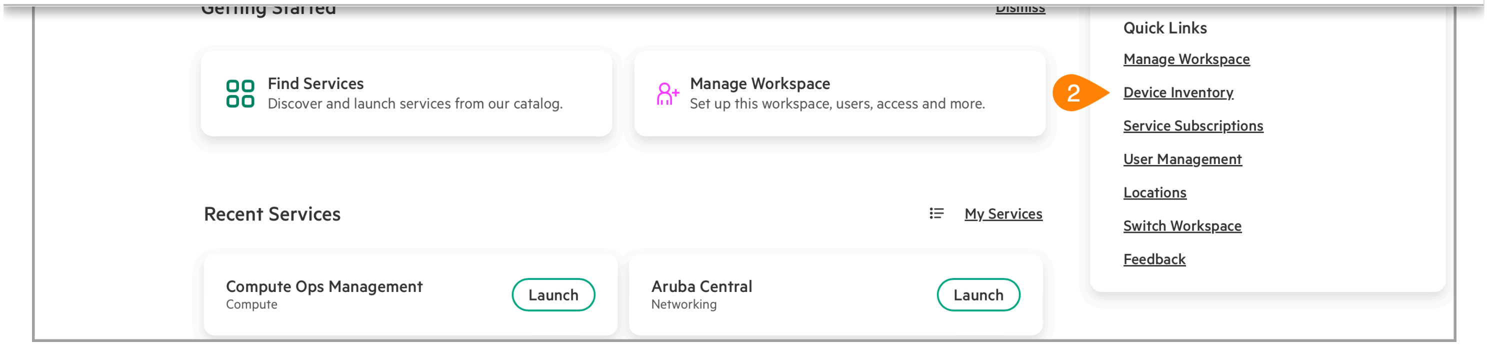


Add Devices to the GreenLake Inventory

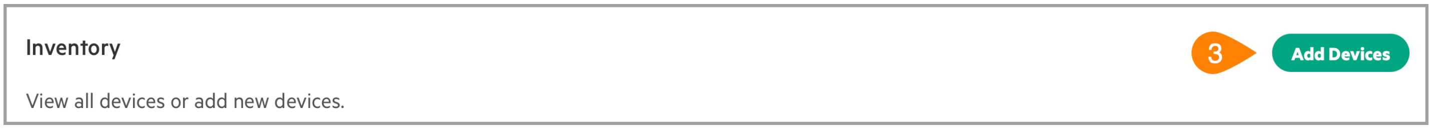
After provisioning Aruba Central, devices are associated to it automatically at the time of purchase. Previously purchased devices can be added manually using the device's serial number and base MAC address. The following procedure demonstrates adding a device manually.

Step 1 Login to GreenLake and select the appropriate Workspace.

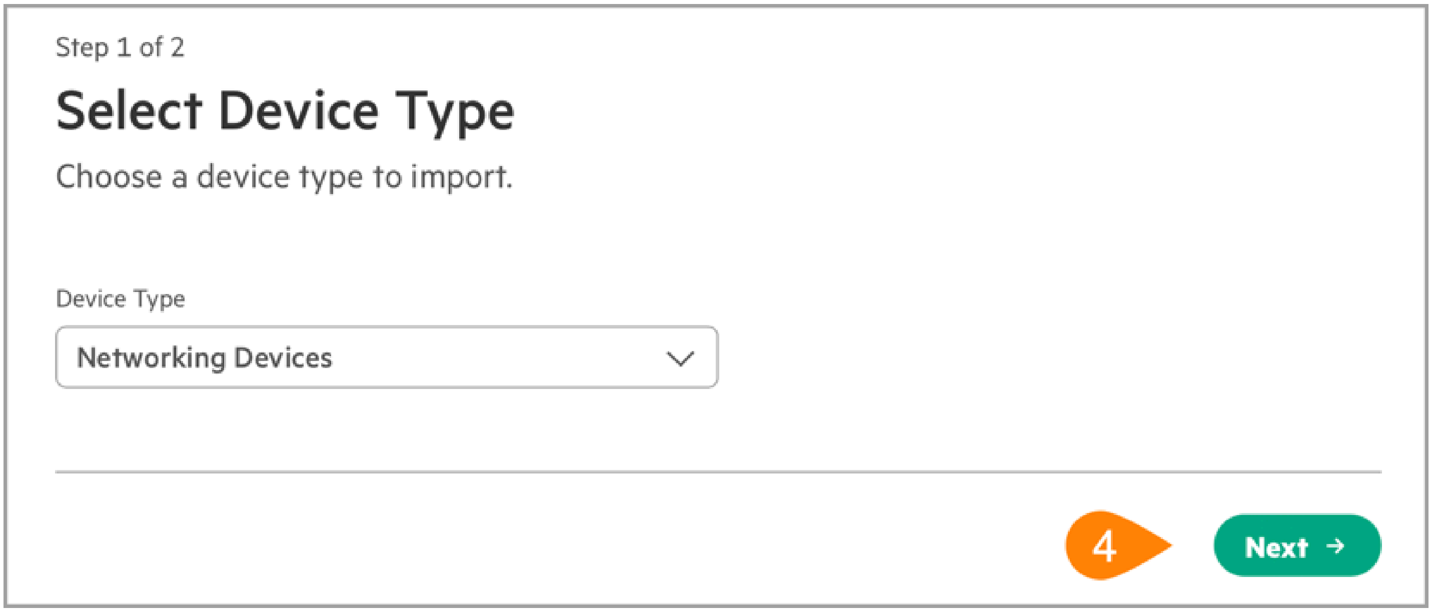
Step 2 On the **Quick Links** menu, click **Device Inventory**.



Step 3 Click **Add Devices**.

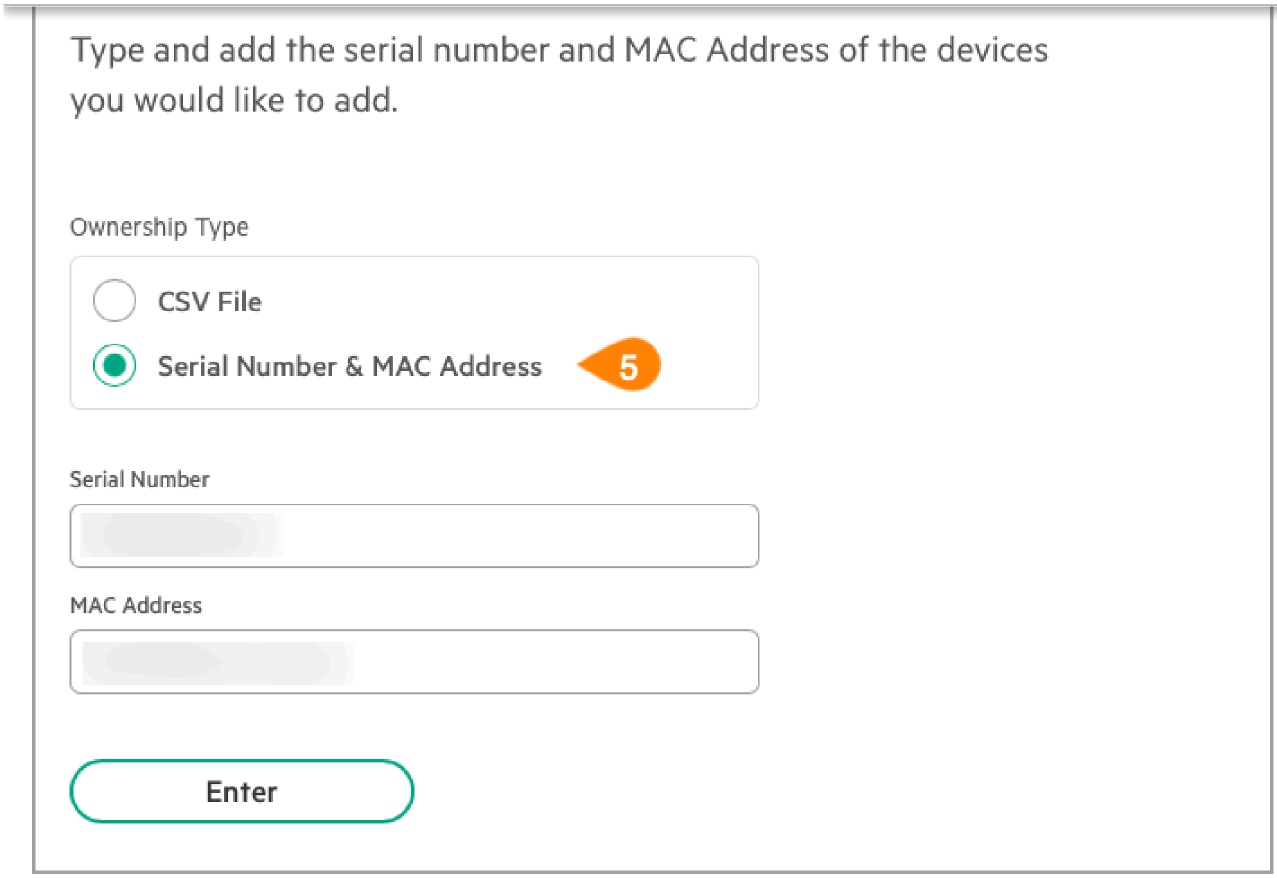


Step 4 Select *Networking Devices* as the **Device Type**. Click **Next**.



Step 5 Click the **Serial Number and MAC Address** radio button. Enter the device's serial number and MAC address. Click **Enter**.

- **Serial Number:** *Device Serial*
- **MAC Address:** *MAC Address*



Type and add the serial number and MAC Address of the devices you would like to add.

Ownership Type

○ CSV File

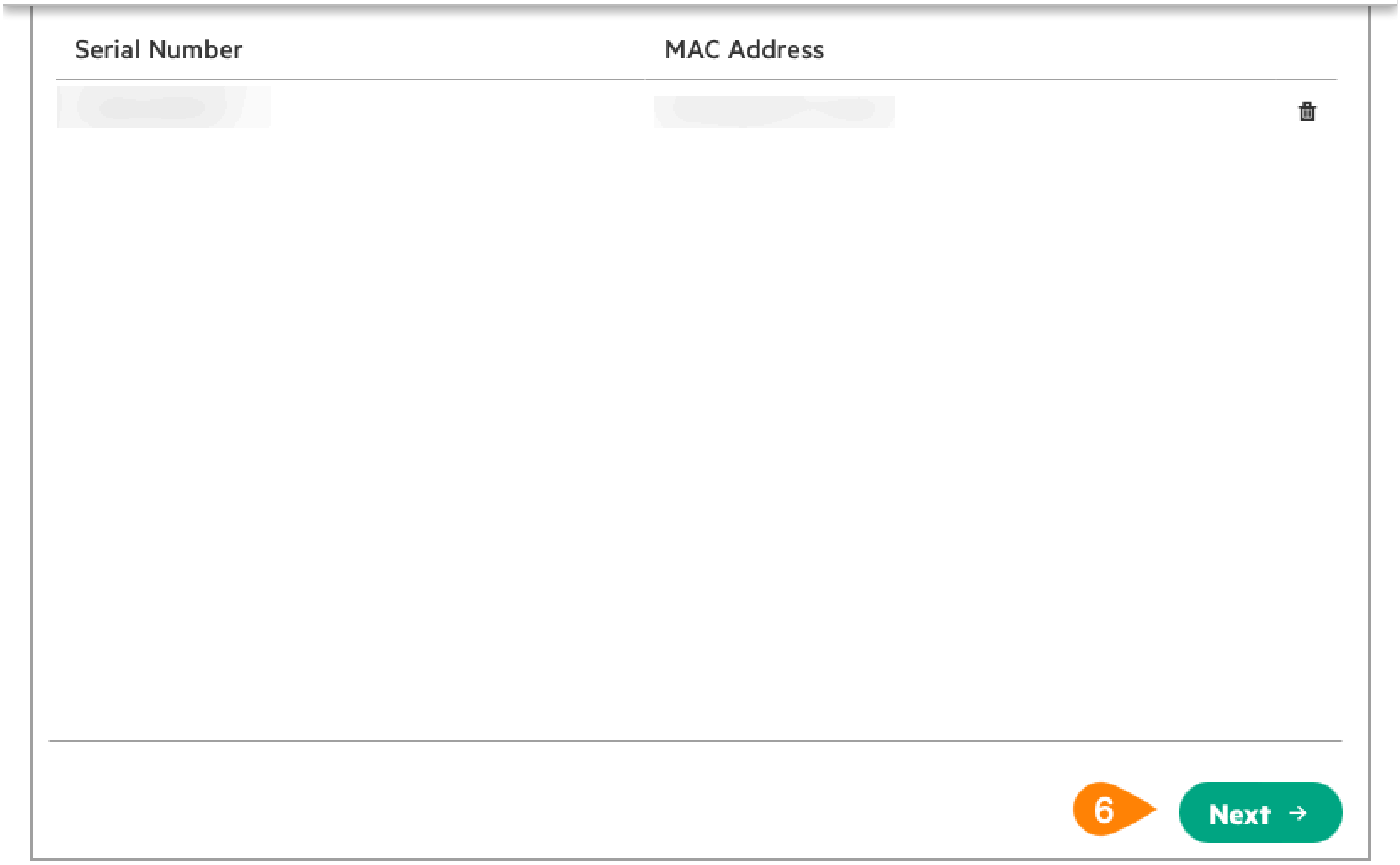
● Serial Number & MAC Address

Serial Number

MAC Address

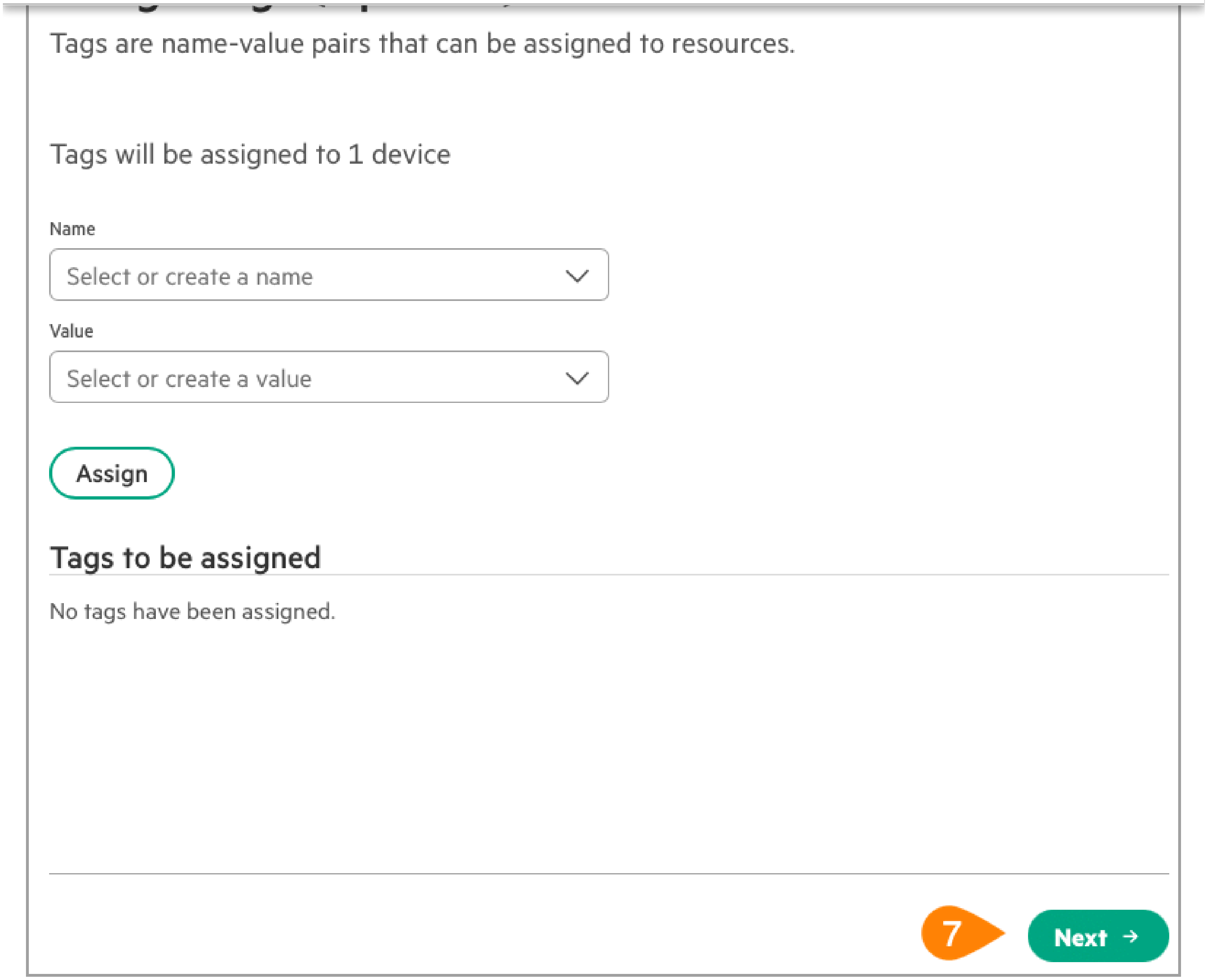
ℹ **Note:** Serial numbers and MAC addresses typically are located on the back or front of a device. The serial number and base MAC address of a CX switch can be displayed using the **show system** CLI command. Execute the **mfginfo** command in apboot mode to see the AP MAC address and serial number.

Step 6 Scroll down to find the device information. Repeat the previous step to add add multiple devices. Click **Next**.



Serial Number	MAC Address	
		🗑

Step 7 Tags are optional. Click **Next**.



Tags are name-value pairs that can be assigned to resources.

Tags will be assigned to 1 device

Name: Select or create a name

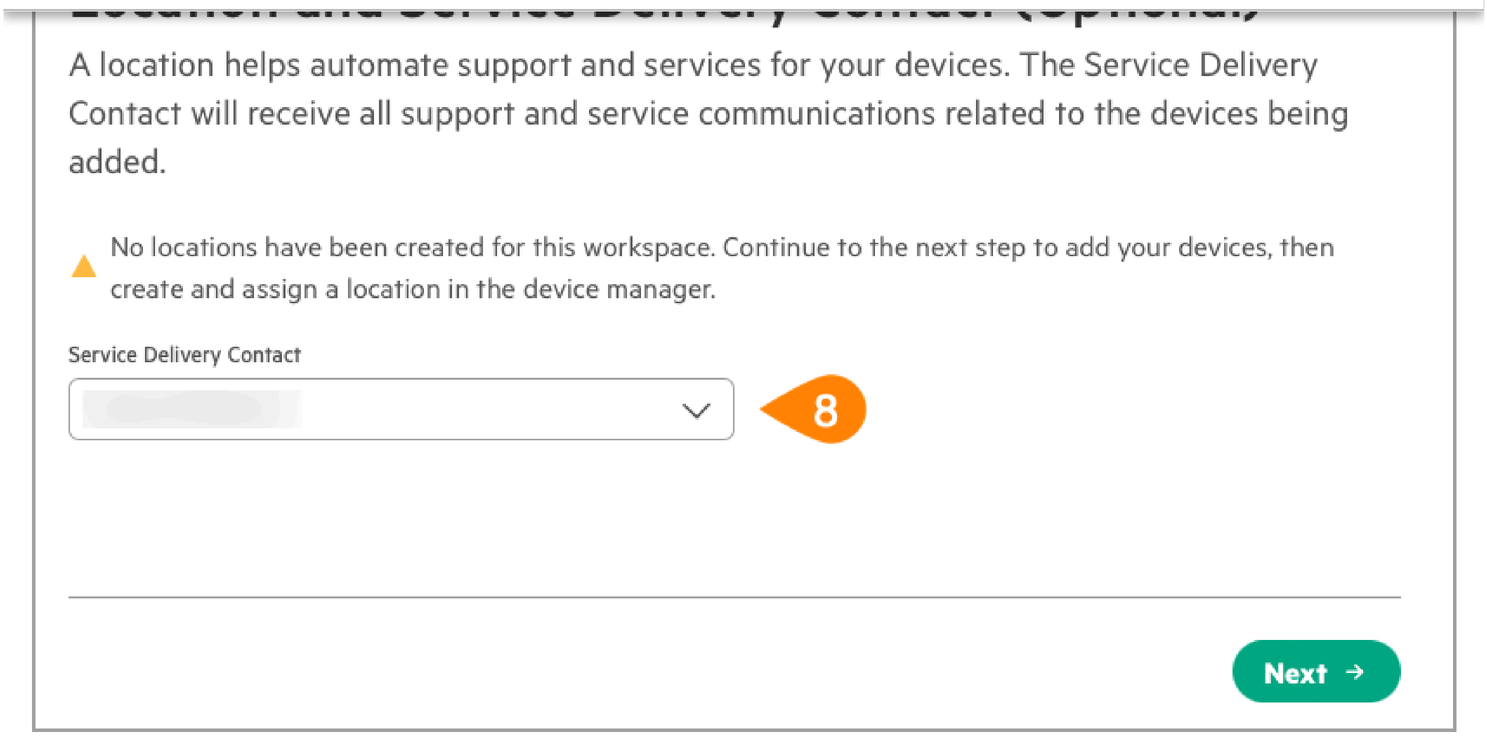
Value: Select or create a value

Tags to be assigned

No tags have been assigned.

Note: Use tags to identify different type of resources, for easier organization and searching.

Step 8 Enter the optional **Service Delivery Contact**. Click **Next**.



Location and Service Delivery Contact (Optional)

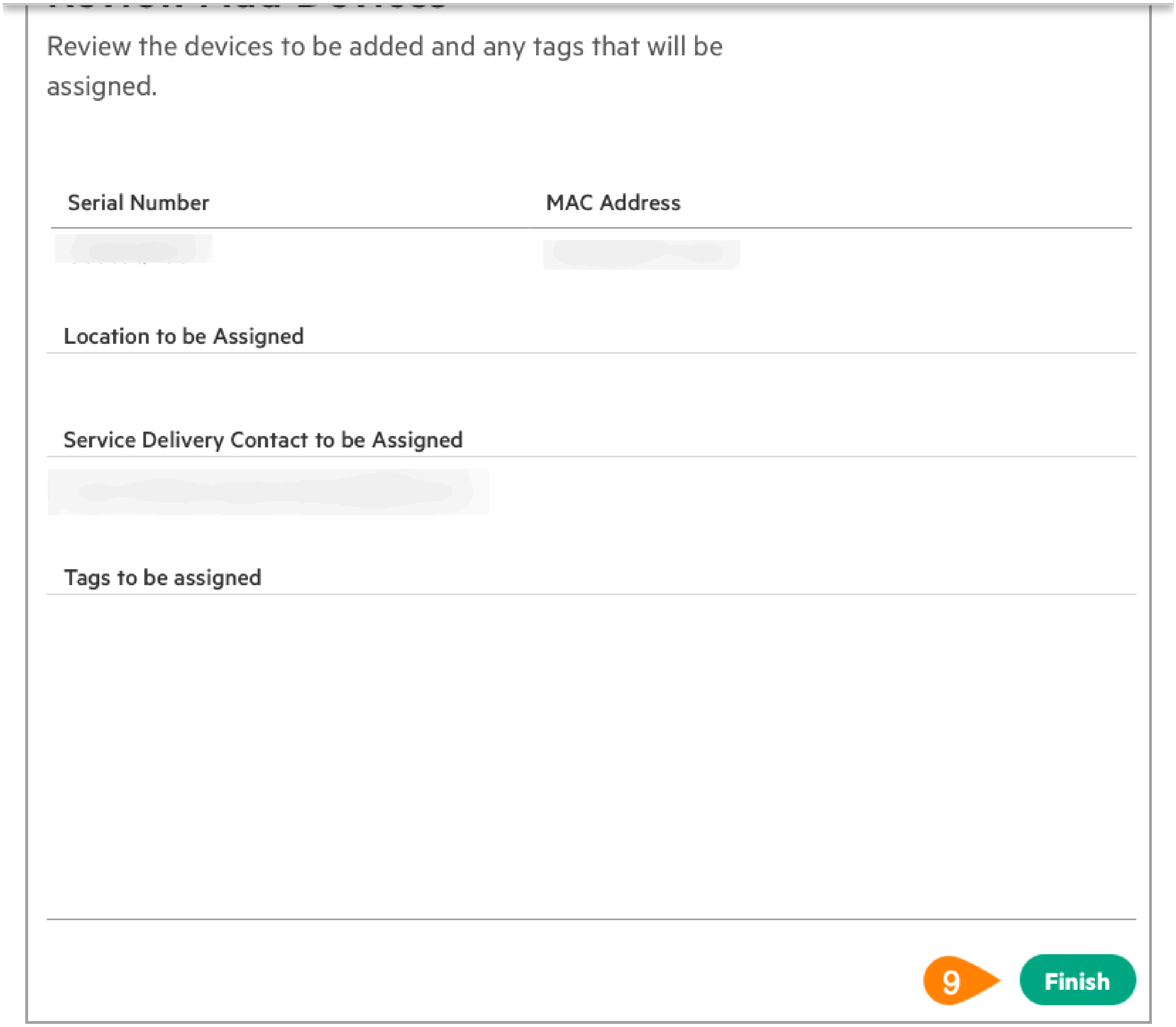
A location helps automate support and services for your devices. The Service Delivery Contact will receive all support and service communications related to the devices being added.

⚠ No locations have been created for this workspace. Continue to the next step to add your devices, then create and assign a location in the device manager.

Service Delivery Contact

Note: Add the location and contact information, if they do not appear in the drop box.

Step 9 Review the list of devices. Click **Finish**.



Review the devices to be added and any tags that will be assigned.

Serial Number	MAC Address
[redacted]	[redacted]

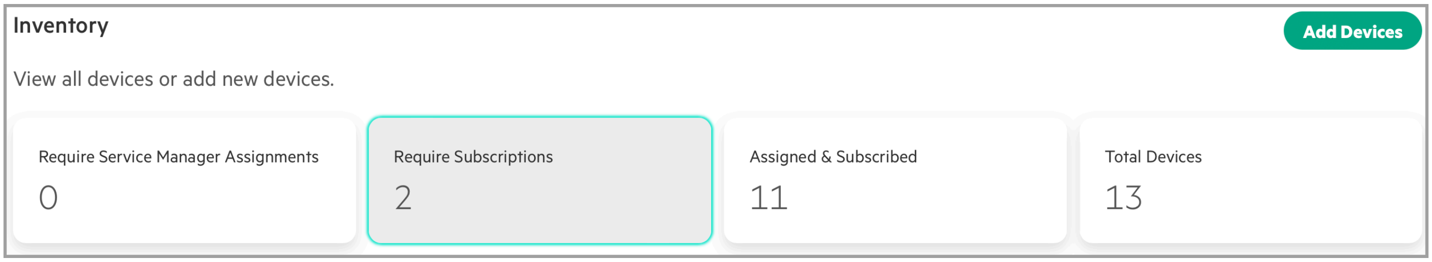
Location to be Assigned

Service Delivery Contact to be Assigned

[redacted]

Tags to be assigned

Step 10 Verify that the devices added to the workspace appear under **Require Subscriptions** in the **Require Service Manager Assignments** tiles.



Inventory

View all devices or add new devices.

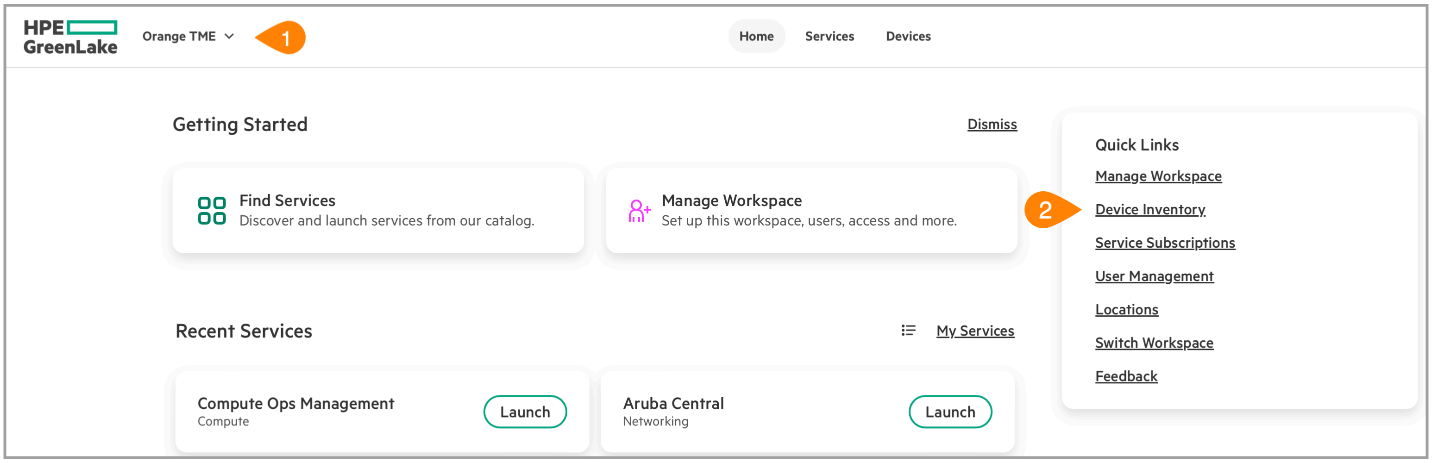
Require Service Manager Assignments	Require Subscriptions	Assigned & Subscribed	Total Devices
0	2	11	13

Add Device Subscription Keys

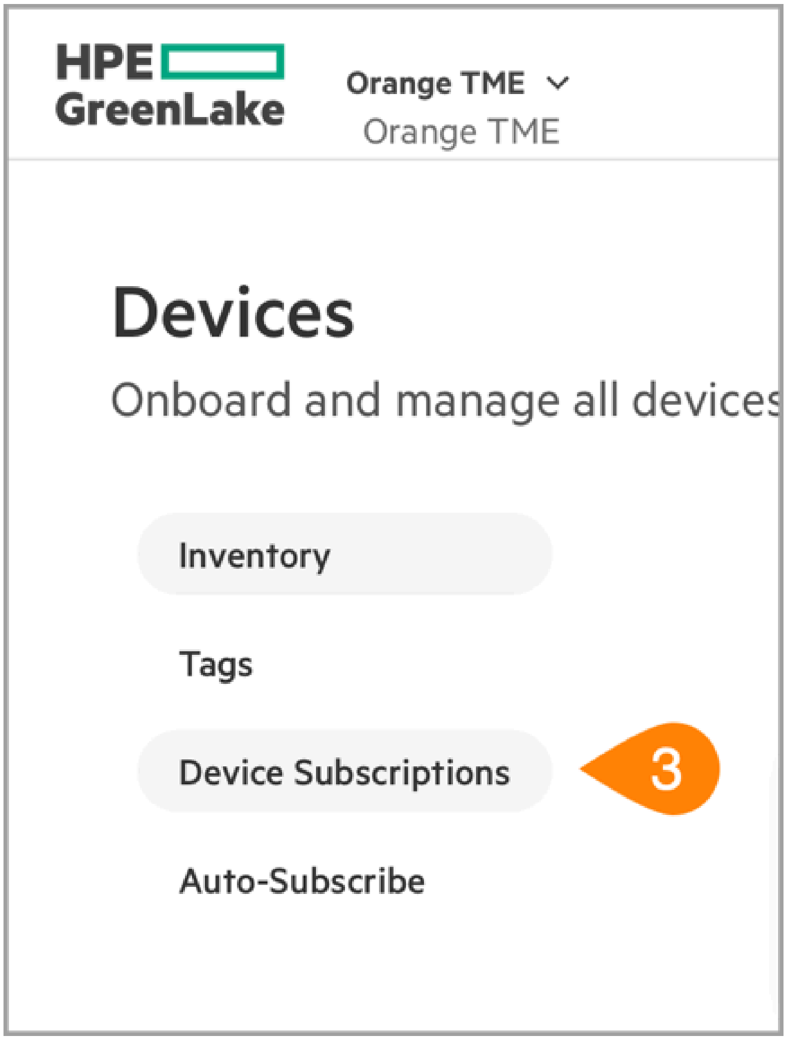
subscription keys in Aruba Central, for subsequent assignment to devices.

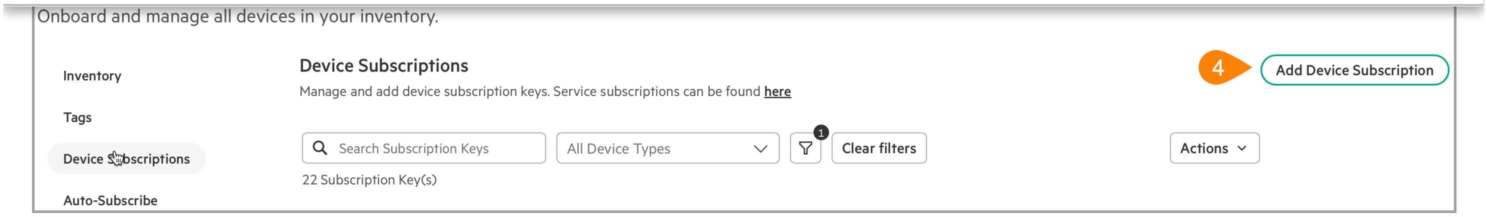
Step 1 Login to GreenLake and select the appropriate Workspace.

Step 2 From the **Quick Links** menu, click **Device Inventory**.



Step 3 In the left menu, click **Device Subscriptions**.





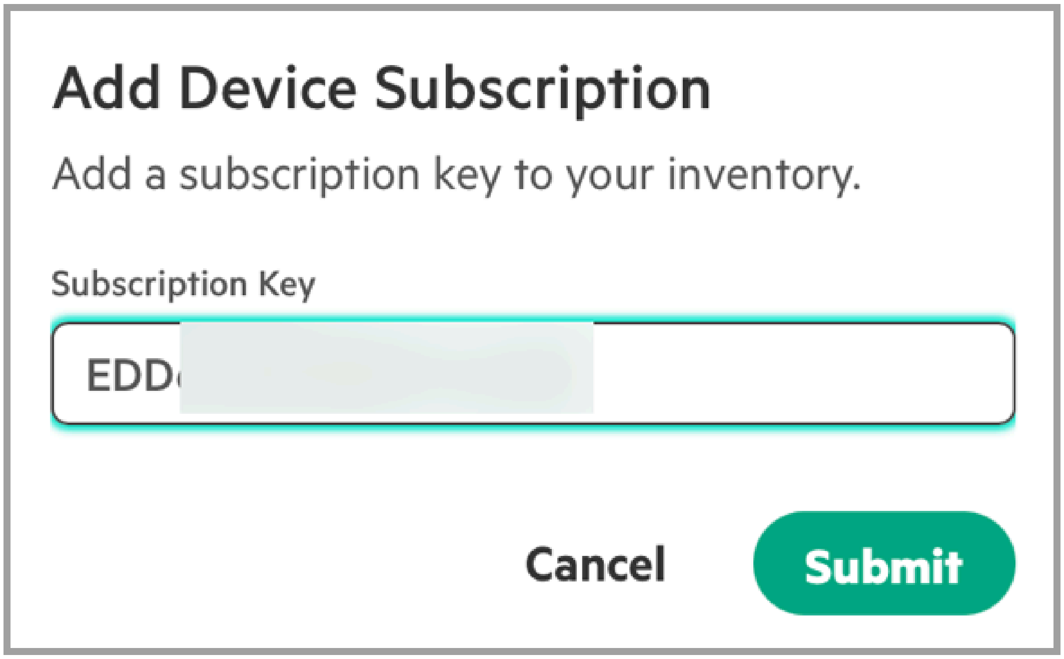
Onboard and manage all devices in your inventory.

Device Subscriptions

Manage and add device subscription keys. Service subscriptions can be found here

22 Subscription Key(s)

Step 5 Enter the device subscription key in the **Add Device Subscription** window. Click **Submit**.



Add Device Subscription

Add a subscription key to your inventory.

Subscription Key: EDD[redacted]

Step 6 Repeat the process to add additional device subscription keys.

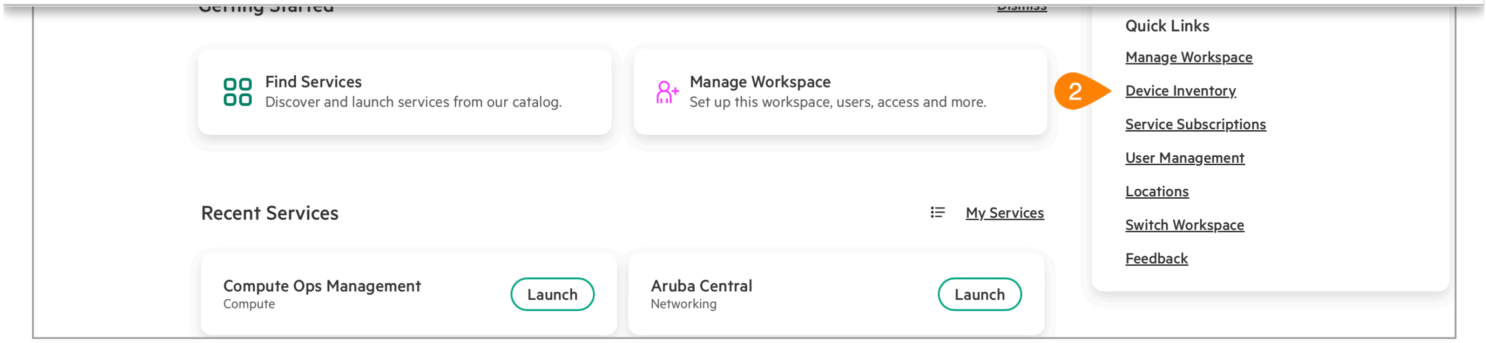
Setup Auto-Subscribe

Auto-subscribe is recommended for managing device subscriptions. Use device subscription tokens to access basic network management services such as monitoring, configuration, and report generation. When a device is added to the HPE GreenLake inventory, the auto-subscribe feature checks for available subscription tokens in the workspace and assigns them to devices automatically. Tokens with the longest available subscription period are assigned first. If the workspace does not have an adequate number of subscriptions, the user may have to assign subscriptions manually to devices as needed. Each device type requires its own auto-subscription configuration.

The following procedure enables auto-subscription.

Step 1 Login to GreenLake and select the Workspace.

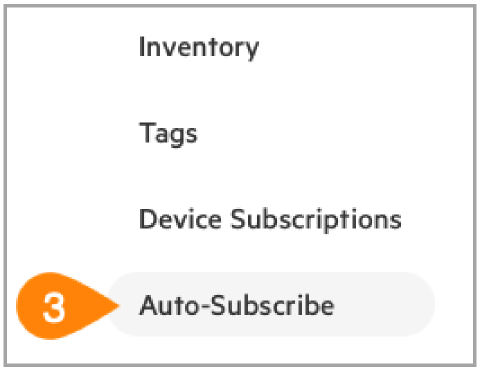
Step 2 On the **Quick Links** menu, click **Device Inventory**.



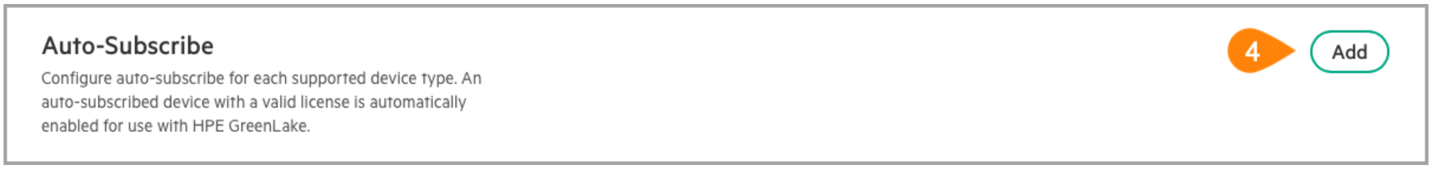
Discover and launch services from our catalog.

Set up this workspace, users, access and more.

Step 3 On the left menu, click **Auto-Subscribe**.

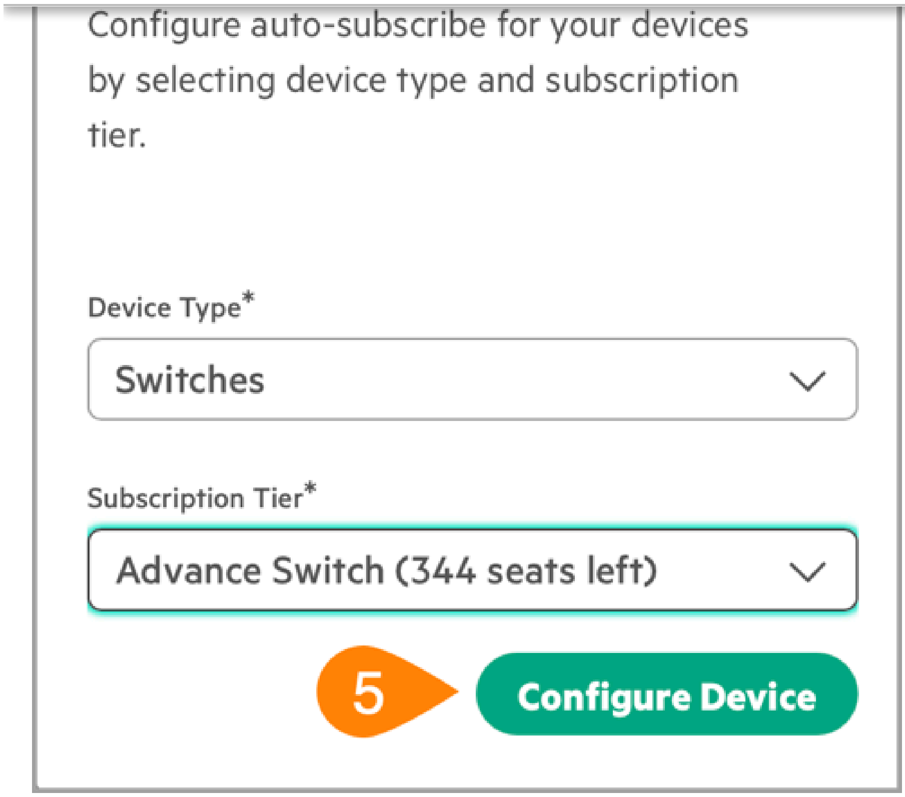


Step 4 Click **Add**.



Configure auto-subscribe for each supported device type. An auto-subscribed device with a valid license is automatically enabled for use with HPE GreenLake.

Step 5 Select the **Device Type** and **Subscription Tier**. Click **Configure Device**.



Configure auto-subscribe for your devices by selecting device type and subscription tier.

Device Type*
Switches

Subscription Tier*
Advance Switch (344 seats left)

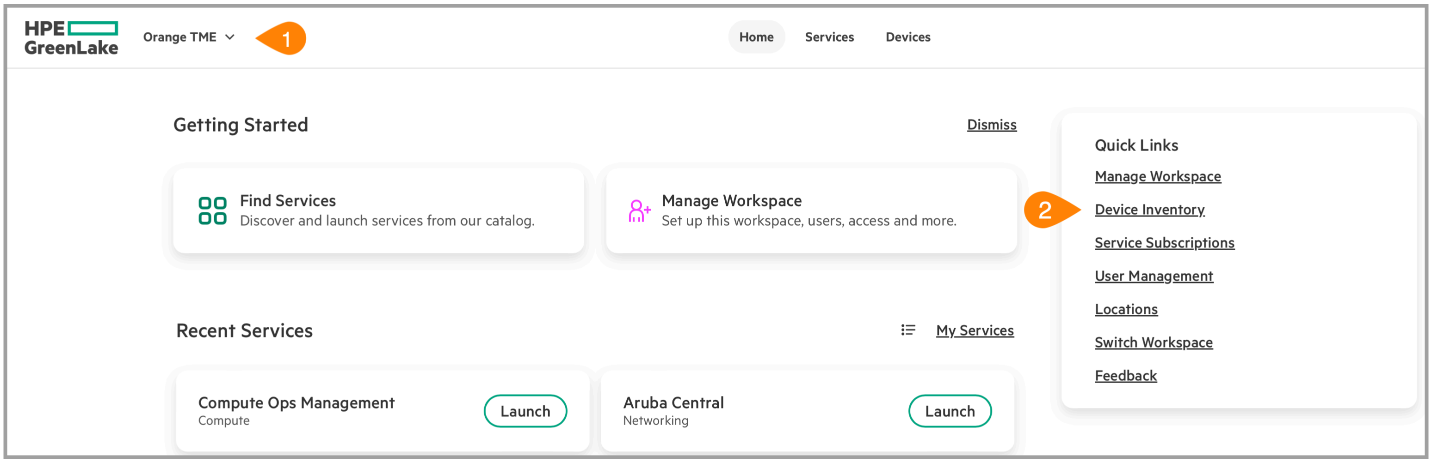
Step 6 Repeat the process to auto-subscribe other device types.

Assign Licenses to Devices Manually

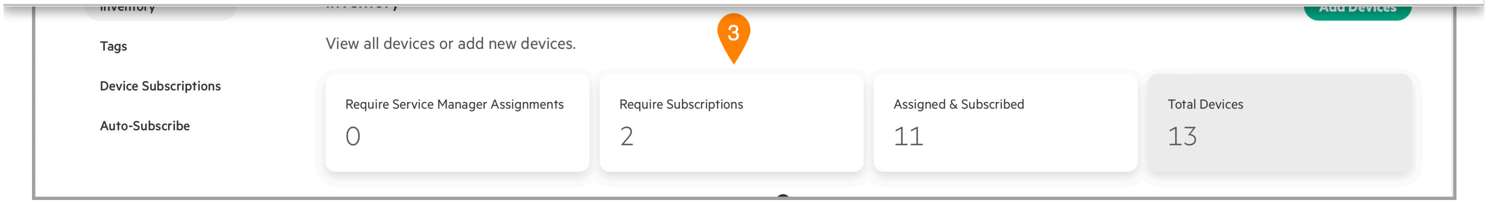
The following procedure assigns device licenses manually. The process can be automated for some device types. Instructions to setup the automated process can be found in the section above.

Step 1 Login to GreenLake and select the appropriate Workspace.

Step 2 From **Quick Links** menu, click **Device Inventory**.



Step 3 Click the **Required Subscriptions** tile.



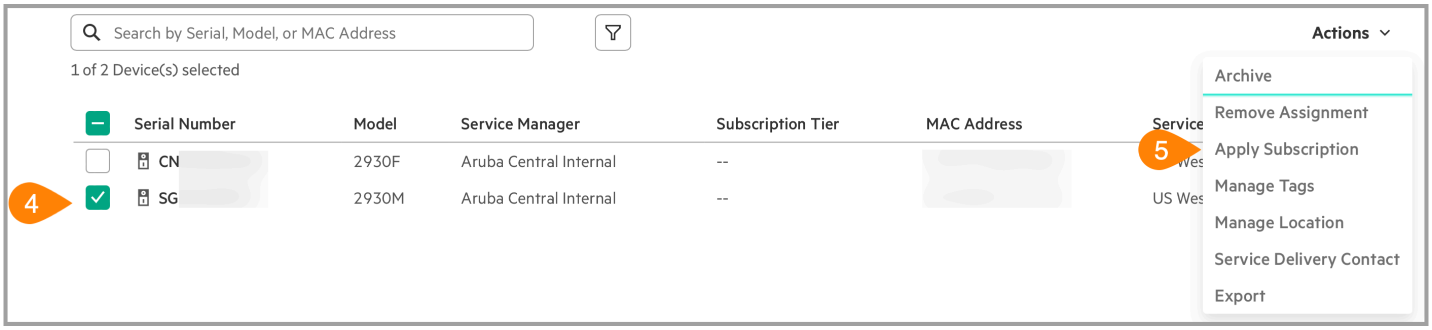
Tags
Device Subscriptions
Auto-Subscribe

View all devices or add new devices.

Require Service Manager Assignments	Require Subscriptions	Assigned & Subscribed	Total Devices
0	2	11	13

Step 4 Select one or more devices using the check box.

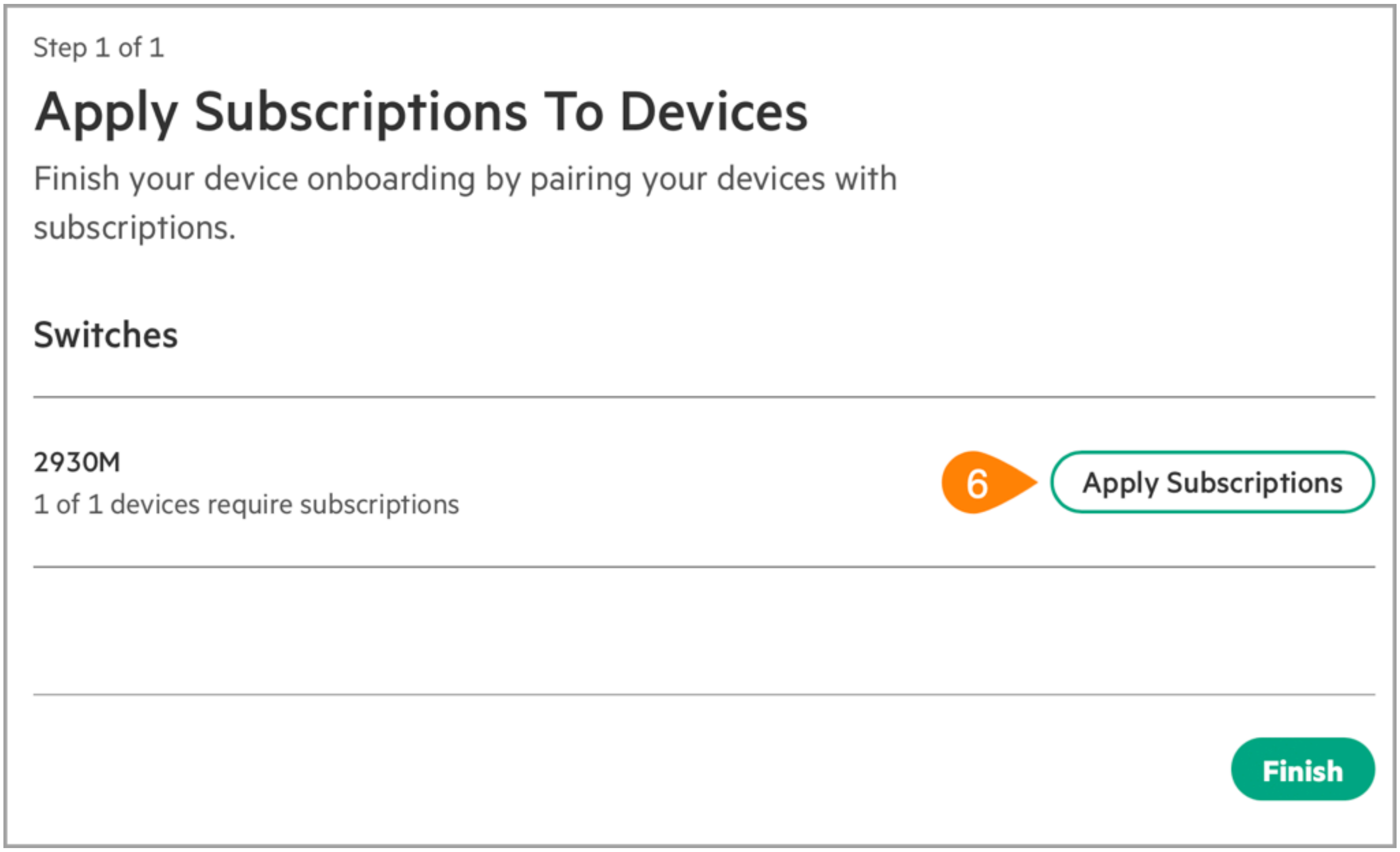
Step 5 In the **Actions** dropdown, select **Apply Subscription**.



1 of 2 Device(s) selected

	Serial Number	Model	Service Manager	Subscription Tier	MAC Address	Service
□	CN[redacted]	2930F	Aruba Central Internal	--	[redacted]	Wes
☑	SG[redacted]	2930M	Aruba Central Internal	--	[redacted]	US Wes

Step 6 Click **Apply Subscriptions**.



Step 1 of 1

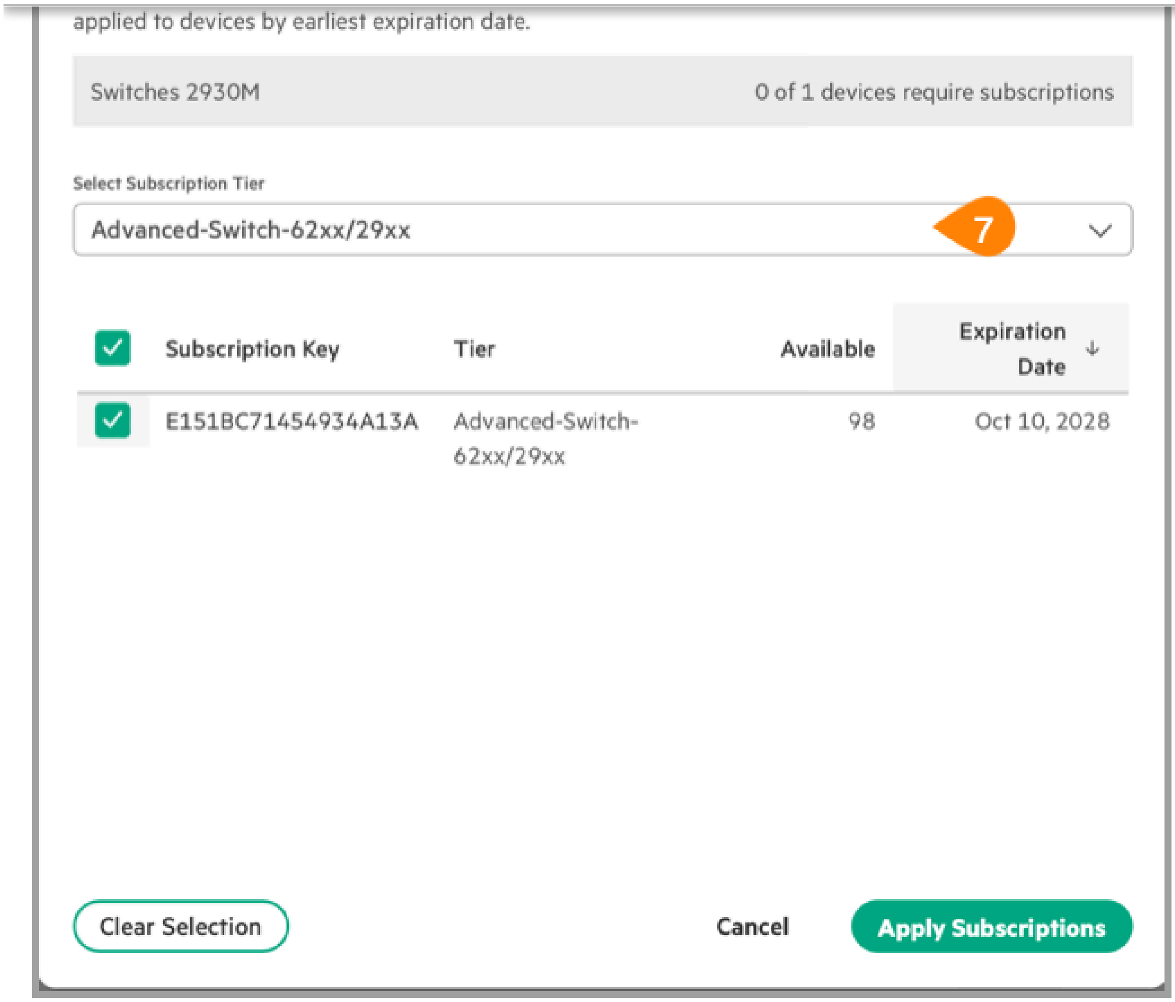
Apply Subscriptions To Devices

Finish your device onboarding by pairing your devices with subscriptions.

Switches

2930M
1 of 1 devices require subscriptions

Step 7 Select the type of subscription in the **Select Subscription Tier** dropdown, check the box for the purchased subscription key, then click **Apply Subscriptions**.



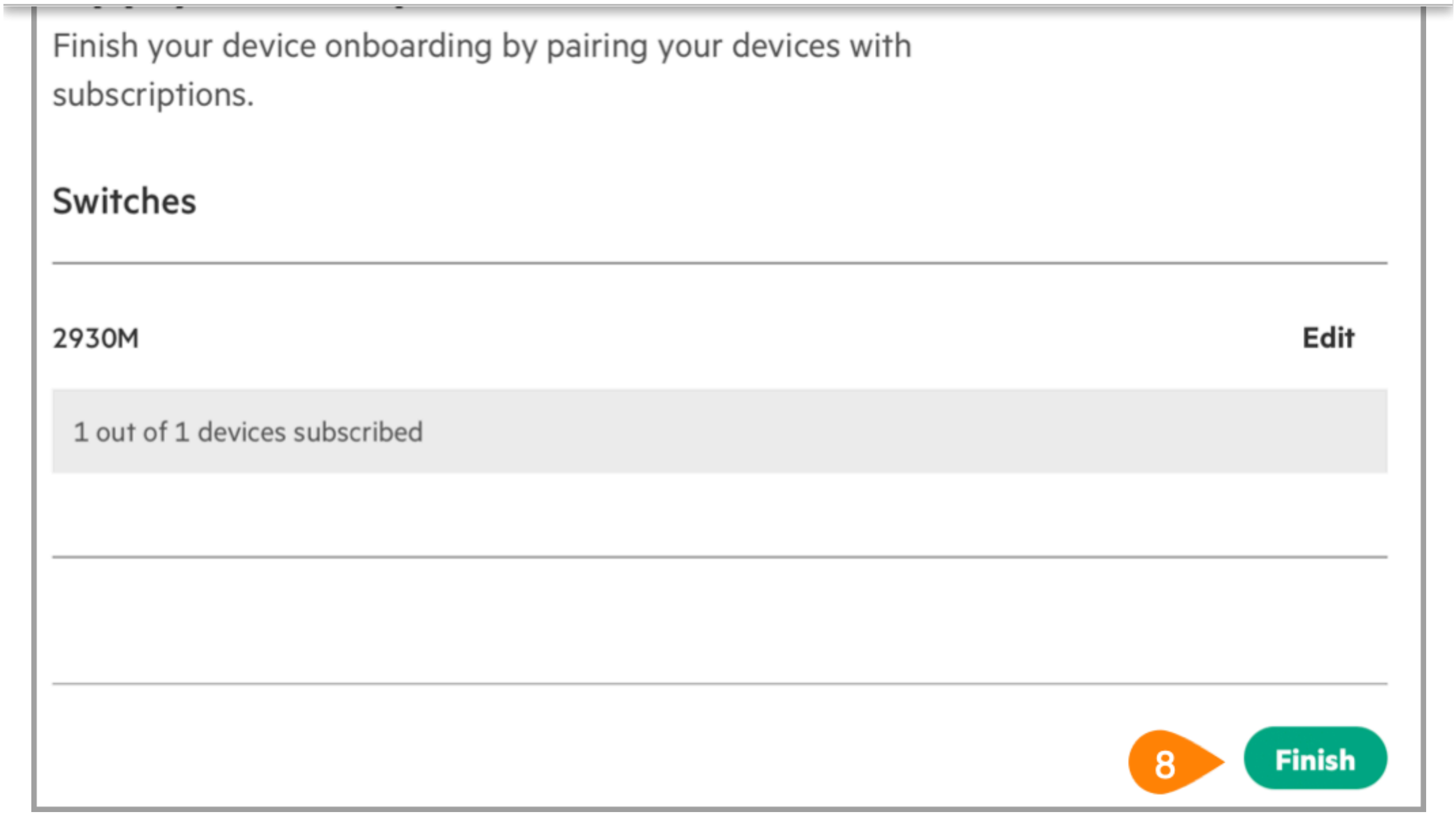
applied to devices by earliest expiration date.

Switches 2930M 0 of 1 devices require subscriptions

Select Subscription Tier: Advanced-Switch-62xx/29xx

☑	Subscription Key	Tier	Available	Expiration Date ↓
☑	E151BC71454934A13A	Advanced-Switch-62xx/29xx	98	Oct 10, 2028

Step 8 Click **Finish**.



Finish your device onboarding by pairing your devices with subscriptions.

Switches

2930M

1 out of 1 devices subscribed

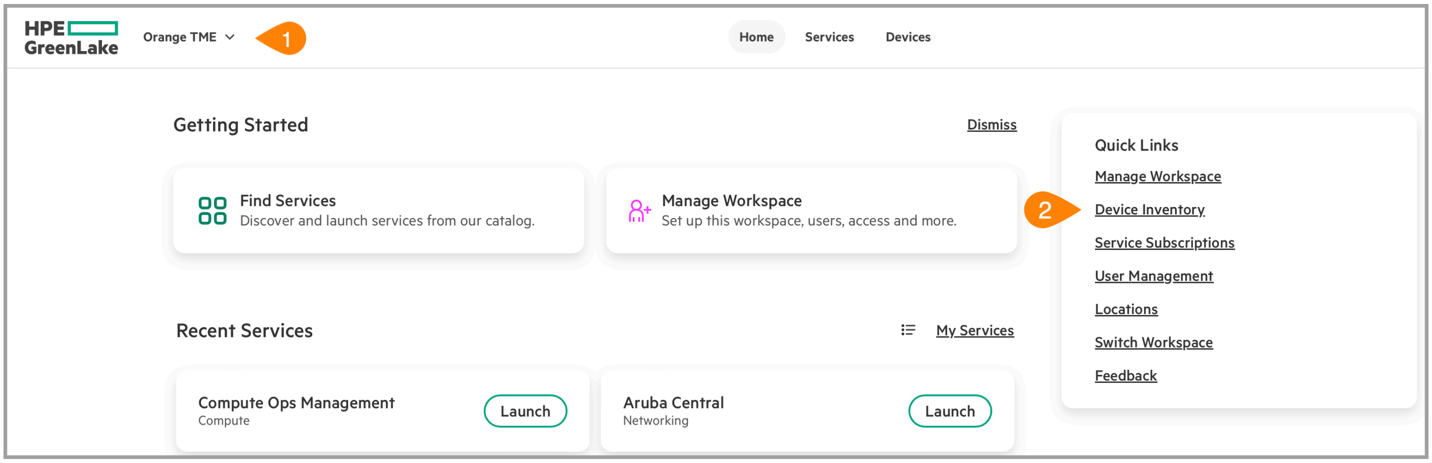
Step 9 Repeat the procedure for all other devices.

Assign Devices to Aruba Central

After a device has been added to GreenLake, it must be assigned manually to an Aruba Central instance. The following procedure assigns a device to the Aruba Central application in HPE GreenLake.

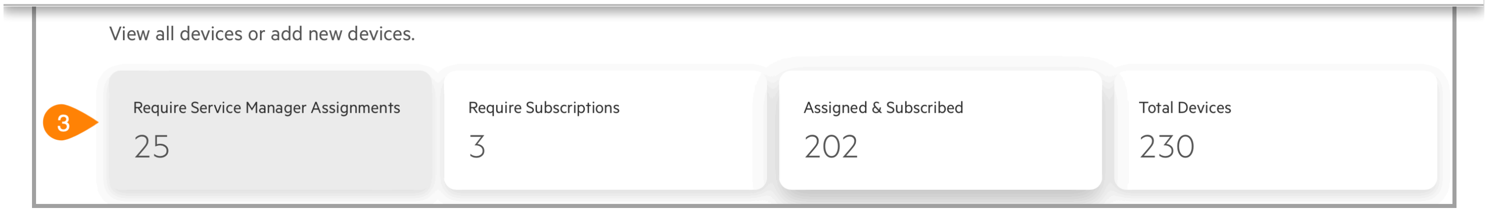
Step 1 Login to GreenLake and select the appropriate Workspace.

Step 2 On the **Quick Links** menu, click **Device Inventory**.



Find Services
Discover and launch services from our catalog.

Manage Workspace
Set up this workspace, users, access and more.

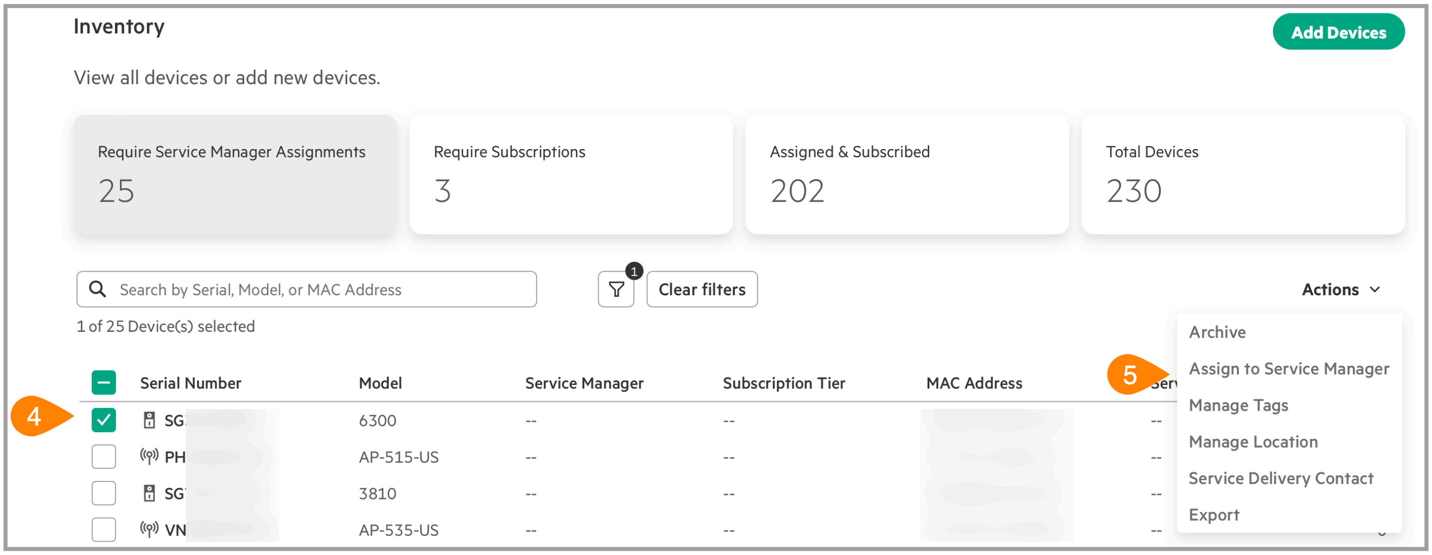


View all devices or add new devices.

Require Service Manager Assignments	Require Subscriptions	Assigned & Subscribed	Total Devices
25	3	202	230

Step 4 Check the box(es) beside one or more devices to assign to Aruba Central.

Step 5 In the **Actions** dropdown, click **Assign to Service Manager**.



Inventory

View all devices or add new devices.

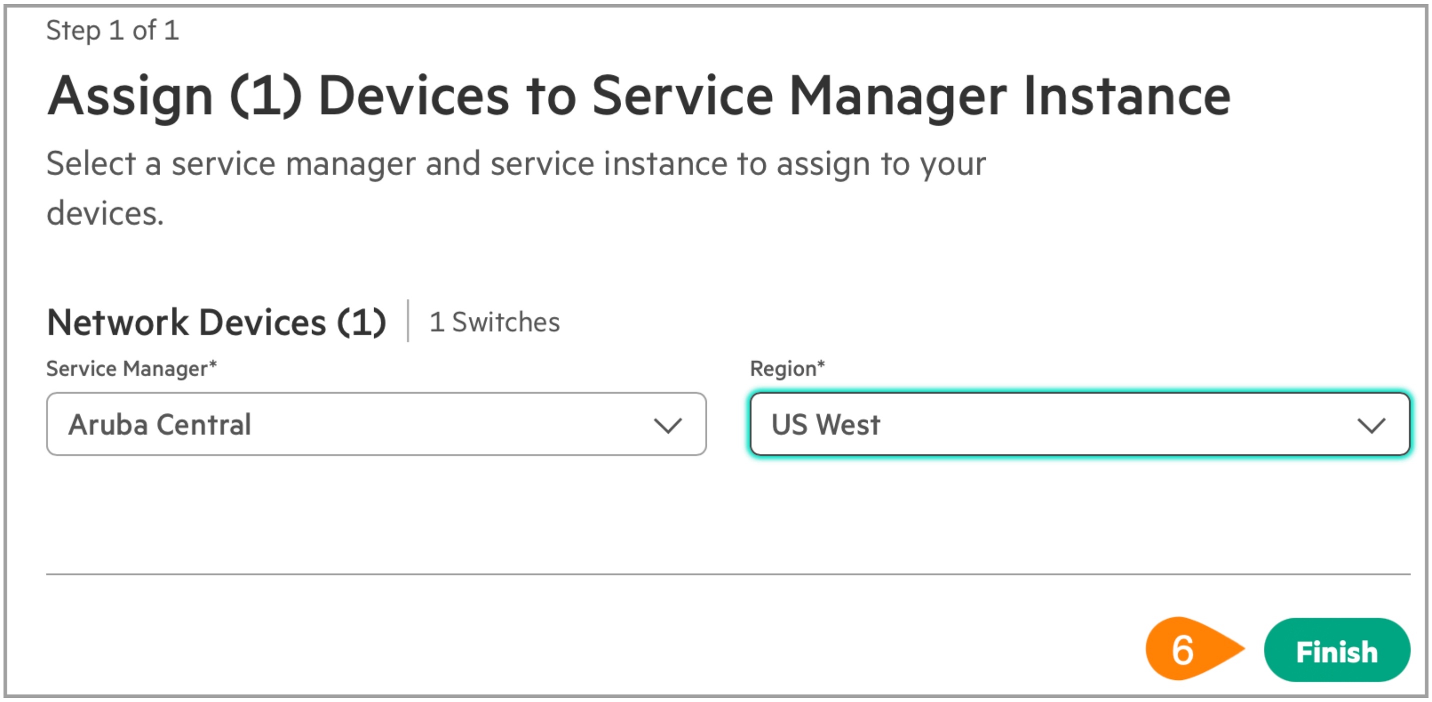
Require Service Manager Assignments	Require Subscriptions	Assigned & Subscribed	Total Devices
25	3	202	230

Search by Serial, Model, or MAC Address

1 of 25 Device(s) selected

	Serial Number	Model	Service Manager	Subscription Tier	MAC Address	Serv
☑	SG[redacted]	6300	--	--	[redacted]	--
□	PH[redacted]	AP-515-US	--	--	[redacted]	--
□	SG[redacted]	3810	--	--	[redacted]	--
□	VN[redacted]	AP-535-US	--	--	[redacted]	--

Step 6 Select **Aruba Central** in the **Service Manager** dropdown and select the desired **Region**. Click **Finish**.



Step 1 of 1

Assign (1) Devices to Service Manager Instance

Select a service manager and service instance to assign to your devices.

Network Devices (1) | 1 Switches

Service Manager*: Aruba Central

Region*: US West

Step 7 Repeat the procedure to assign more devices to Aruba Central.

REFERENCE 2

Hewlett Packard
Enterprise

Become a Member

Community Home | Discussion 4.5K | Members 1.2K

View Only

Back to discussions

Expand all | Collapse all

sort by thread

Aruba Central Is Now Part of HPE GreenLake

This thread has been viewed 449 times

C ClarenceHillard2 Mar 18, 2022 01:31 PM

With the upcoming 2.5.5 software release, Aruba Central will become integrated with the HPE GreenLake ...

I IL20 May 09, 2022 12:38 PM

Hello Clarence, Thank you for such a good post with all the detailed information regarding Aruba Central ...

1. Aruba Central Is Now Part of HPE GreenLake

3 Kudos

C

ClarenceHillard2

Posted Mar 18, 2022 01:31 PM

Edited by ClarenceHillard2 Mar 30, 2022 12:26 PM

Reply | Reply Privately

Become a Member

With the upcoming 2.5.5 software release, Aruba Central will become integrated with the HPE GreenLake edge-to-cloud platform. Read the following post for a quick overview of HPE GreenLake, how this development will benefit your IT organization, what Aruba Central features have moved as a result of this effort, and where you can find more information regarding these changes.

What is HPE GreenLake?

HPE GreenLake provides a unified platform for viewing and managing compute, storage, and networking infrastructure from HPE and Aruba. So rather than having separate management consoles and login screens for each of your IT domains, HPE GreenLake delivers a common view, with a consistent operating model across edge, data center, colocation, and multi-cloud environments – improving IT efficiency while providing tighter control over all of your infrastructure.

How Does This Benefit My Organization?

By integrating Aruba Central with HPE GreenLake, IT admins will now have a global view to manage users, policies, subscriptions, the audit trail, and device inventories across various regions from the same account, in the same dashboard as other HPE products (e.g., data services and compute).

Specifically, this development will deliver the following benefits for customers:

Higher IT efficiency with a single place to view and manage network infrastructure alongside HPE data and compute services.

Tighter security via the HPE GreenLake single sign-on and embedded audit trail.

Improved cost controls with consumption analytics across all infrastructure to help optimize spend and ensure investments are utilized as intended.

A better IT experience through a more responsive Aruba Central user interface.

How Will This Change the Admin Experience in Aruba Central?

The following account management functions, which were previously located on the Account Home page of the Aruba Central user interface, will now be viewed and managed from the HPE GreenLake portal.

App Catalog – Find and deploy new applications within the customer's organization (e.g., compute, storage)

Onboard Devices – Add and assign devices in the customer's device inventory (network, compute, and storage)

Subscriptions – View and assign subscriptions to available devices

Users and Roles – Add new users and assign or modify pre-built or custom roles and permissions

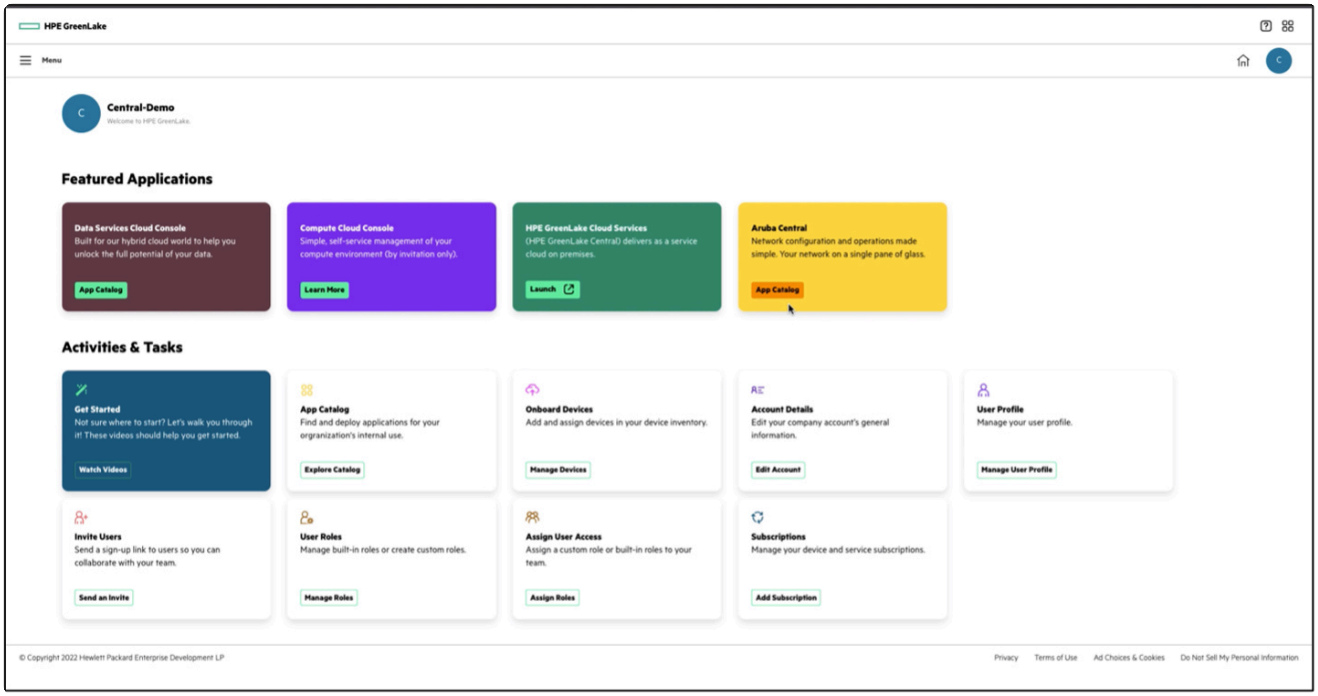
Audit Trail – Logs all account-level changes in a single audit trail

Single Sign-On – Access all HPE and Aruba workloads from a single portal

Become a Member

For more information about using these features on HPE GreenLake, see the HPE GreenLake User Guide. You can also watch our walkthrough videos for an overview of how to execute these workflows within HPE GreenLake.

To access Aruba Central's network health dashboards and management GUI, network operators simply launch Aruba Central via the HPE GreenLake dashboard, as depicted below.



Central-Demo

Welcome to HPE GreenLake.

Featured Applications

Data Services Cloud Console
Built for our hybrid cloud world to help you unlock the full potential of your data.
App Catalog

Compute Cloud Console
Simple, self-service management of your compute environment (by invitation only).
Learn More

HPE GreenLake Cloud Services
(HPE GreenLake Central) delivers as a service cloud on premises.
Launch

Aruba Central
Network configuration and operations made simple. Your network on a single pane of glass.
App Catalog

Activities & Tasks

Get Started
Not sure where to start? Let's walk you through it! These videos should help you get started.
Watch Videos

App Catalog
Find and deploy applications for your orgranization's internal use.
Explore Catalog

Onboard Devices
Add and assign devices in your device inventory.
Manage Devices

Account Details
Edit your company account's general information.
Edit Account

User Profile
Manage your user profile.
Manage User Profile

Invite Users
Send a sign-up link to users so you can collaborate with your team.
Send an Invite

User Roles
Manage built-in roles or create custom roles.
Manage Roles

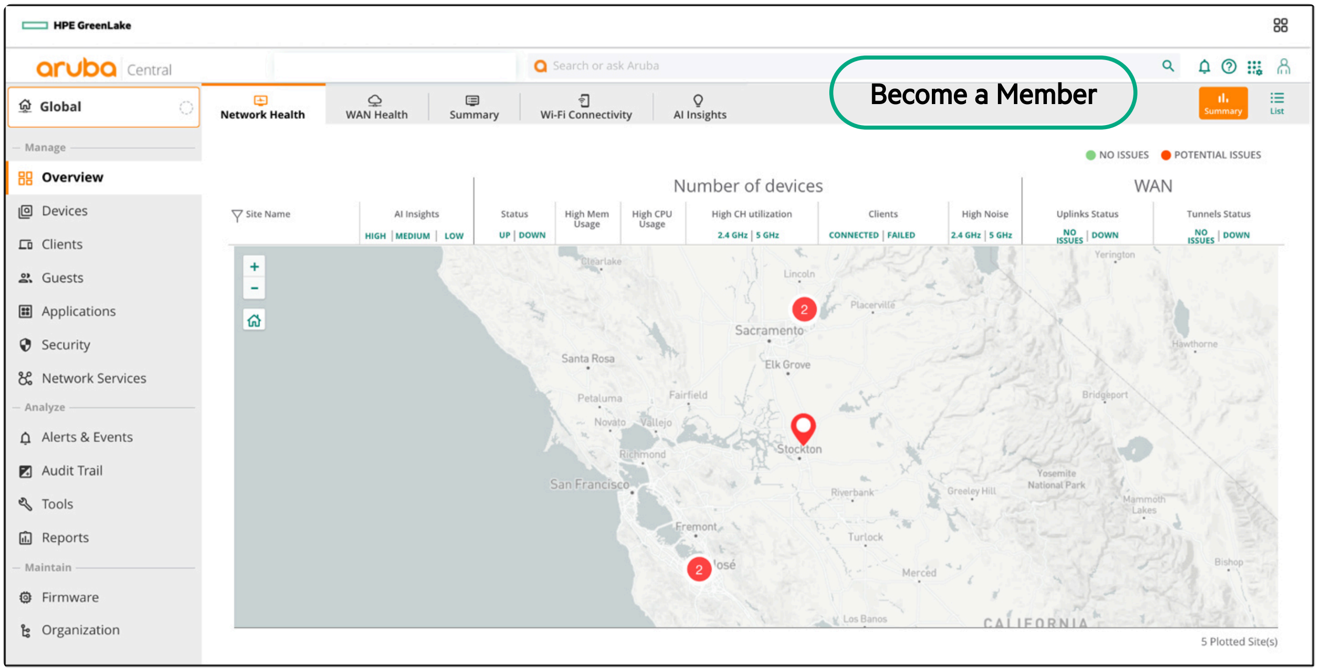
Assign User Access
Assign a custom role or built-in roles to your team.
Assign Roles

Subscriptions
Manage your device and service subscriptions.
Add Subscription

© Copyright 2022 Hewlett Packard Enterprise Development LP

Privacy Terms of Use Ad Choices & Cookies Do Not Sell My Personal Information

Upon clicking on the Aruba Central tile in the application catalogue, the primary user interface that network admins are familiar with will load in their web browser, now embedded under a common "HPE GreenLake" banner, as shown below. All network configuration, monitoring, and troubleshooting functions follow the same menus and workflows – no additional learning curve or new skills required.

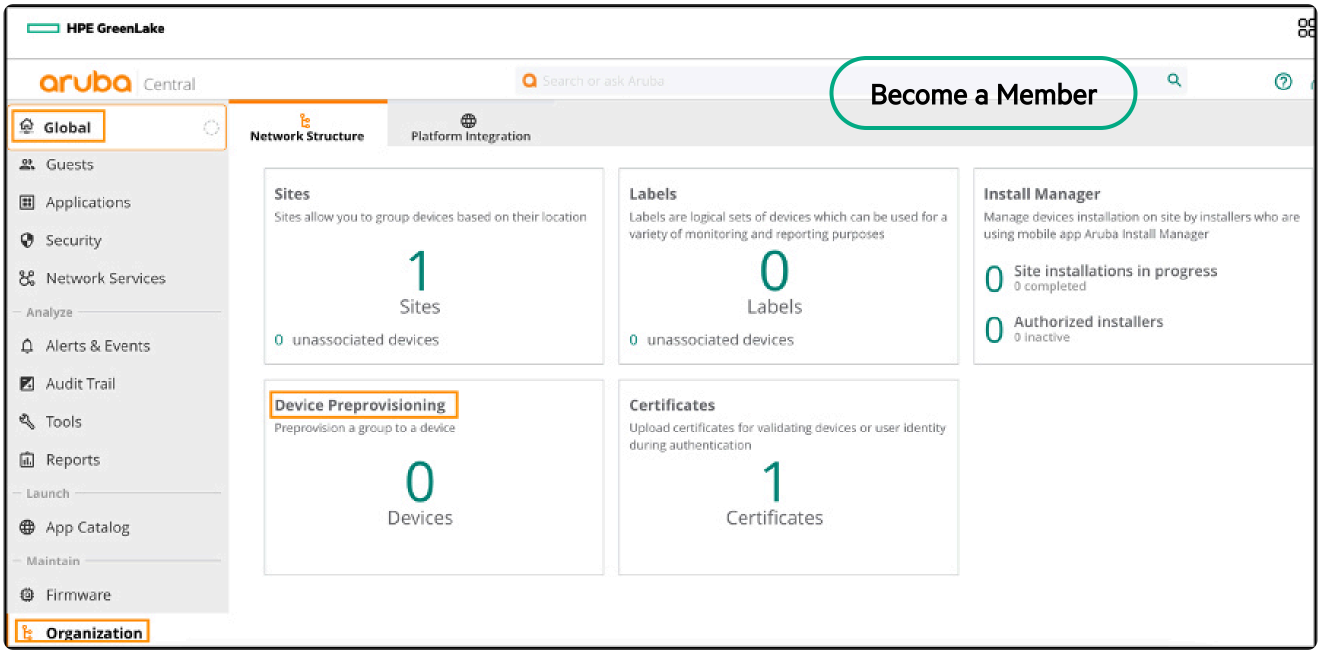


What Functions Have Changed Within Aruba Central?

The following functions have moved to a new location within the existing Aruba Central user interface

Assigning newly added devices to groups
Data Collectors
API Gateway
Streaming API
Webhooks

See the below screenshots for a representative view of where these functions will be located within Aruba Central moving forward.



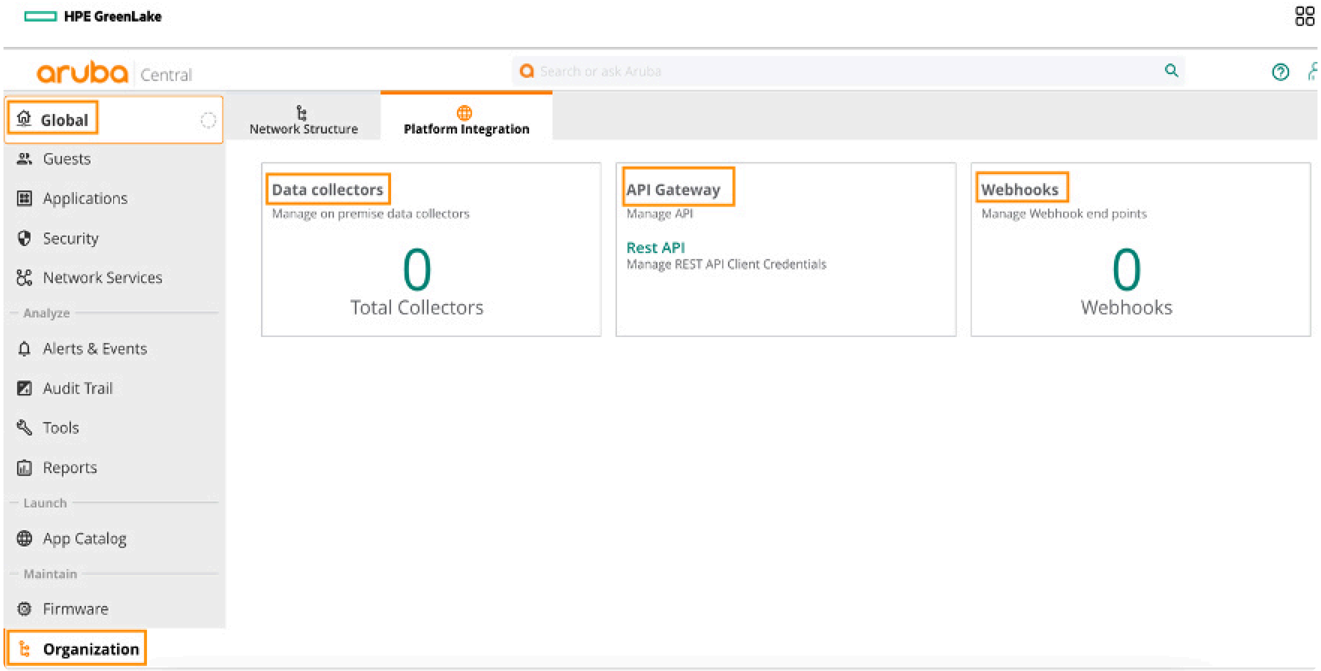
Sites
Sites allow you to group devices based on their location
1
Sites
0 unassociated devices

Labels
Labels are logical sets of devices which can be used for a variety of monitoring and reporting purposes
0
Labels
0 unassociated devices

Install Manager
Manage devices installation on site by installers who are using mobile app Aruba Install Manager
0 Site installations in progress
0 completed
0 Authorized installers
0 inactive

Device Preprovisioning
Preprovision a group to a device
0
Devices

Certificates
Upload certificates for validating devices or user identity during authentication
1
Certificates



Data collectors
Manage on premise data collectors
0
Total Collectors

API Gateway
Manage API
Rest API
Manage REST API Client Credentials

Webhooks
Manage Webhook end points
0
Webhooks

View more details on where to access these features by visiting the Aruba Central Help Center.

Note: All Aruba Central customer data (devices, configuration, users, reports and all other data) will be migrated as-is during the HPE GreenLake integration.

Become a Member

Accessing HPE GreenLake

HPE GreenLake is accessible at https://common.cloud.hpe.com.

Aruba customers are not required to create an HPE GreenLake account. Existing Aruba Central accounts will be mapped to a GreenLake account.

When will these changes take effect?

These changes will take effect once your Aruba Central production cluster migrates to the 2.5.5 code release. Production clusters will start migrating to Aruba Central 2.5.5 in mid-March 2022. At that point, there is a rolling schedule of availability based on the location of the customer's Central production cluster. It is expected that by April 30, 2022, all customers worldwide will have access to Central 2.5.5 functionality and the new experience within HPE GreenLake.

Additional Resources

Please refer to the following resources to learn more about Aruba Central within HPE GreenLake.

HPE GreenLake Resources: Getting Started with GreenLake | GreenLake user guide
Aruba Central Help Center*: Aruba Central 2.5.5 Home Page | What's New for Central 2.5.5
Aruba Central on HPE GreenLake: Walkthrough Videos
Aruba Support Advisories: Aruba Support Portal

* The online help guide will continue to be updated with new information leading up to the general availability of the Aruba Central 2.5.5 software release. Please bookmark the page and check back periodically for the latest information

Become a Member

Clarence Hillard
----

2. RE: Aruba Central Is Now Part of HPE GreenLake

1 Kudos

I

IL20

Posted May 09, 2022 12:38 PM

Reply Reply Privately

Hello Clarence,

Thank you for such a good post with all the detailed information regarding Aruba Central with HPE GreenLake.

I have a question: Do you know where HPE GreenLake servers are hosted? If so, is there any information?

Thank you in advance!

Iker Lineo
Channel SE
HPE Aruba
Spain | Barcelona

› Original Message

RELATED CONTENT

Become a Member

Central Audit Trail and Configuration User

victorcastro
Added Nov 24, 2021

Discussion Thread **4**

Okta for SSO with HPE GreenLake (and Aruba Central)

ProbeRequest
Added Dec 20, 2022

Discussion Thread **2**

Add Devices to Aruba Central Group from HPE Greenlake

parkerma Added Sep 21, 2022

Discussion Thread **4**

Okta for SSO with HPE GreenLake (and Aruba Central)

ProbeRequest
Added Dec 20, 2022

Library Entry

Unwanted/unused HPE GreenLake workspaces

Steinar Grande
Added Jul 24, 2023

Discussion Thread **3**

Hewlett Packard Enterprise | Airheads Community

Contact

WW Corporate Headquarters -
Spring, TX - United States
1701 E Mossy Oaks Rd
Spring, TX 77389

Company

About Us

Careers

Contact Us

Environmental Citizenship

Privacy policy

Terms of service

Support

Support Services

Contact Support

Training & Certification

Software Downloads

Licensing Login

Partners

Find a Partner

Become a Partner

Partner Ready for Networking

Technology Partner Programs

Legal

Become a Member

Powered by Higher Logic

REFERENCE 3

Legal Disclaimer: The resource assets in this website may include abbreviated and/or legacy terminology for HPE Aruba Networking products. See www.arubanetworks.com for current and complete HPE Aruba Networking product lines and names.

Search

You are here: Home > About Aruba Central

About Aruba Central

Aruba Central is a powerful cloud networking solution that offers simplicity for today's networks. As the management and orchestration console for Aruba ESP (Edge Services Platform), Aruba Central provides a single point of control to oversee all aspects of wired and wireless LANs, WANs, and VPNs across campus, branch, and remote office locations.

AI-powered analytics, end-to-end orchestration and automation, and advanced security features are built into the solution. Live upgrades, robust reporting, and live chat support are also included, bringing more efficiency in day-to-day maintenance activities.

Built on a cloud-native, micro services architecture, Aruba Central delivers on enterprise requirements for scale and resiliency, but is also driven by intuitive workflows and dashboards that make it a perfect fit for SMBs with limited IT personnel. So, whether you have one business location or several, IT can spend less time on managing network infrastructure and more time on creating value for the business.

Key Features

Listed below are some of the key features of Aruba Central:

- Unified management of wireless, wired, VPN, and SD-WAN for simplified operations.
- AI-based insights for faster troubleshooting and continuous network optimization.
- Integration with Aruba UXI to proactively monitor and improve the end-user experience.
- Advanced IDS/IPS threat defense management.
- Powerful monitoring and troubleshooting for remote or home office networks.
- APIs and webhooks for ease of integration with other leading IT platforms.

- Live Chat and an AI-based search engine for an enhanced support experience.
- SaaS, on-premises, and managed service options for flexible consumption and financing.

Central Key Terms

Before getting started with configuring, it is important to understand some important configuration concepts and terminology. The following topics are discussed in this section:

- **Cluster Zone**—Refers to an deployment area within a specific region. In other words, cluster zones are regional grouping of one or more container instances on which is deployed. Cluster zones allow your deployments to restrict customer data to a specific region and plan time zone specific maintenance windows. Each cluster zone has separate URLs for signing up for , accessing portal, and for allowing devices to communicate with . To view the zone in UI, click the User Settings menu at the bottom of the left navigation pane.
- **Enterprise Mode**—Refers to the solution deployment mode in which the customers provision, manage, and maintain their networks end-to-end for their respective organizations or businesses.
- **Managed Services Mode**—Refers to the deployment mode in which the service providers, resellers, administrators, and retailers to centrally manage and monitor multiple tenant or end-customer accounts from a single management interface.
- **Evaluation Account**—Refers to the account created for evaluating solution and its services.
- **Paid Subscriber**—Refers to the customers who have purchased a subscription to obtain access to and its services.
- **Customer ID**—Refers to the identity number of your account.
- **Zero Touch Provisioning**—Refers to one of the following:Zero Touch Provisioning (ZTP) of accounts— When you purchase a subscription key and add this subscription key in , queries the Activate database to retrieve the devices mapped to your purchase order and add these devices to the inventory. This process is referred to as zero touch provisioning in .Zero Touch Provisioning of Devices—Most devices support self-provisioning; that is, when you connect a device to a provisioning network, it can automatically download provisioning parameters from the Activate server and connect to their management entity.
- **Onboarding**—You can view, manage, and onboard all the devices in your account using the Devices option in HPE GreenLake platform.

Getting Started with Aruba Central

Viewing Configuration Status in Aruba Central

Supported Devices

Managing the Overall Network

AI Insights Dashboard

Using the Search Bar

- For more information, see the **Devices** section in the HPE GreenLake Edge to Cloud Platform User Guide.

- **Device Sync**—Refers to the process of synchronizing devices from the Activate database. The device sync operation allows to retrieve devices from Activate and automatically add these devices to the device inventory in .

- **Provisioning**—Refers to the process of setting up a device for deploying networks as per the configuration requirements of your organization.

- **Group**—Refers to the device configuration container in . You can combine devices with common configuration requirements into a single group and apply the same configuration to all the devices in that group.

- **Site**— Refers to the physical locations where devices are installed. Organizing devices per sites allows you to filter your dashboard view per site.

- **Label**—Refers to the tags used for logically grouping devices based on various parameters such as ownership, specific areas within a site, departments, and so on.

- **Standard Enterprise mode**—Refers to the deployment mode in which customers manage their respective accounts end-to-end. The Standard Enterprise mode is a single-tenant environment for a single end-customer.

- **MSP mode**—Refers to the deployment mode in which service providers centrally manage and monitor multiple tenant accounts from a single management interface.

- **Tenant accounts**—End-customer accounts created in the mode. Each tenant is an independent instance of .

- **MSP administrator**—Refers to owners of the primary account. These users have administrator privileges to provision, manage, and monitor tenant accounts.

- **Tenant users**—Refers to the owners of an individual tenant account provisioned in the mode. The administrator can create a tenant account.

- **SSIDs**—Wireless networks are identified using a service set identifier (SSID). The SSIDs distinguish a wireless network from other networks configured within a WLAN boundary. Aruba uses the SSIDs of APs to orchestrate and configure a number of management policies. For more information, see About Aruba Central.

- **Traffic Forwarding Modes**—Depending on the type of WLAN setup, the SSIDs are also used to specify the traffic forwarding modes. ArubaOS 10 supports automated workflows to set up these SSID profiles. For more information, see About Aruba Central.

Getting Started with Aruba Central

Viewing Configuration Status in Aruba Central

Supported Devices

Managing the Overall Network

AI Insights Dashboard

Using the Search Bar

- **Supported Authentication Methods**—In creating the SSID profiles in the automated workflows, you must specify an authentication method. ArubaOS 10 supports a number of authentication methods and each is recommended for a specific deployment type. For more information, see About Aruba Central.

- **Supported Encryption Methods**—In creating the SSID profiles in the automated workflows, you must specify an encryption method. ArubaOS 10 supports a number of encryption methods and each is recommended for a specific deployment type. For more information, see About Aruba Central.

- **Cloud-Assisted Roaming Services**—The Cloud-Assisted Roaming Services feature facilitates fast roaming of 802.11r and Opportunistic Key Caching (OKC) clients, to enable seamless roaming with minimal or no disruption to the application traffic such as voice and video. For more information, see About Aruba Central.

- **Cloud-Assisted Roaming Services**—The Cloud-Assisted Roaming Services feature facilitates fast roaming of 802.11r and Opportunistic Key Caching (OKC) clients, to enable seamless roaming with minimal or no disruption to the application traffic such as voice and video. For more information, see About Aruba Central.

- **Access Rules and Firewall Policies**—The Access Control List (ACL) is a logic that handles stateless inspection of traffic. An ACL is used in many types of implementations including routing policies and user policies. A firewall is a device that performs stateful inspection of traffic (checks for encapsulation) passing through a part of the network and decides whether to allow or deny the traffic. You can configure both ACLs and firewall policies on APs and Gateways. For more information, see About Aruba Central.

- **User Roles and VLANs**—A client connecting to a WLAN SSID that is broadcast by an AP is assigned a user role or VLAN to define the client's network privileges, the frequency of re-authentication, and the applicable bandwidth contracts. For more information, see About Aruba Central.

- **Supported Device Configuration Methods in Aruba Central**—In order to configure the management layer, Aruba Central supports a number of configuration options that includes UI workflows, templates, and APIs. For more information, see Device Configuration Methods in Aruba Central.

Device Configuration Methods in Aruba Central

Aruba Central offers the following options for configuring devices in your account:

Getting Started with Aruba Central

Viewing Configuration Status in Aruba Central

Supported Devices

Managing the Overall Network

AI Insights Dashboard

Using the Search Bar

- **Groups**—You can use the Groups feature to create a logical subset of devices. If you have devices that must share common configuration settings, ensure that you assign these devices to the same group. Any new device joining a group inherits the configuration that is already applied on the devices in a group.
- **Device-specific configuration**—If you have fewer devices that do not have the same configuration requirements, you can apply configuration changes at the device level. In some cases, although the devices are assigned to a group, you may want to have a slightly different configuration on one specific device in a group. In such cases, you can modify the device configuration and apply changes at the device level.
- **Configuration templates**—You can also leverage the configuration templates feature to quickly deploy. To use a template-based configuration method for APs, ensure that you enable the template-based configuration mode when creating AP groups.
- **APIs**—Allow you to configure and monitor devices using NB APIs.

Operational Modes and Interfaces

Aruba offers the following variants of the Aruba Central web interface:

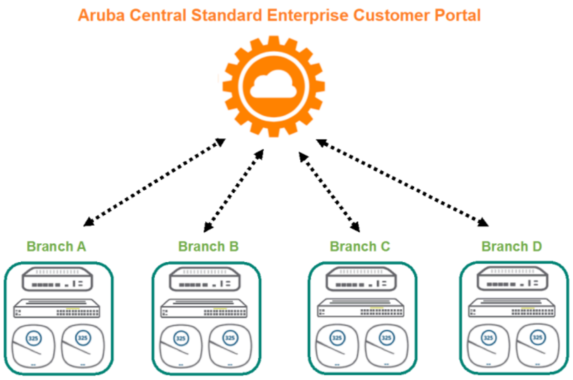
- Standard Enterprise Mode
- Managed Service Provider Mode

Standard Enterprise Mode

Users can manage their respective accounts using the Standard Enterprise interface. In the Standard Enterprise mode, the customers have complete access to their accounts. They can also provision devices and subscriptions to manage their respective accounts.

The following figure illustrates a typical Standard Enterprise mode deployment.

Figure 1 *Standard Enterprise Mode*



Managed Service Provider Mode

Getting Started with Aruba Central

Viewing Configuration Status in Aruba Central

Supported Devices

Managing the Overall Network

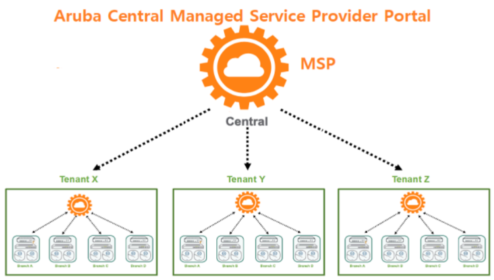
AI Insights Dashboard

Using the Search Bar

Aruba Central offers the MSP mode for managed service providers who must manage multiple customer networks. The MSP administrators can provision tenant accounts, allocate devices, assign licenses, and monitor tenant accounts and their networks. The administrators can also drill down to a specific tenant account and perform administration and configuration tasks. Tenants can access only their respective accounts, and only those features and application services to which they have subscribed.

The following figure illustrates a typical MSP mode deployment.

Figure 2 *Managed Service Provider Mode*



Getting Started with Aruba Central

Viewing Configuration Status in Aruba Central

Supported Devices

Managing the Overall Network

AI Insights Dashboard

Using the Search Bar

[Reference 3]

REFERENCE 4

Search

You are here: Home > Getting Started > Accessing Aruba Central Portal

Accessing Aruba Central Portal

After you create an Aruba Central account, the link to Aruba Central portal will be sent to your registered email address. You can use this link to log in to Aruba Central.

If you are accessing the login URL from the www.arubanetworks.com website, ensure that you select the zone in which your account was created.

This section includes the following topics:

- Login URLs
- Logging in to Aruba Central
- Changing Your Password
- Logging Out of Aruba Central

Login URLs

When you try to access Aruba Central portal, you are redirected to the Aruba Central URL that is mapped to your cluster zone.

Table 1: *Cluster Zone— Portal URLs*

Regional Cluster	Sign Up URL
US-1	https://portal.central.arubanetworks.com/signup
US-2	https://portal-prod2.central.arubanetworks.com/signup OR https://signup.central.arubanetworks.com/
Canada-1	https://portal-ca.central.arubanetworks.com/signup
China-1	https://portal.central.arubanetworks.com.cn/signup
EU-1	https://portal-eu.central.arubanetworks.com/signup
APAC-1	https://portal-apac.central.arubanetworks.com/signup
APAC-EAST1	https://portal-apaceast.central.arubanetworks.com/signup
APAC-SOUTH1	https://portal-apacsouth.central.arubanetworks.com/signup

Logging in to Aruba Central

To log in to Aruba Central:

1. Access the Aruba Central login URL for your zone.
2. Notice that the zone is automatically selected based on your geographical location.
3. Enter the email address and click **Continue**.
4. Log in using your credentials.

NOTE

If your user credentials are stored in your organization's Identity Management server and SAML SSO authentication is enabled for your IdP on Aruba Central, complete the SSO authentication workflow. For more information on SAML configuration, see Solution Overview

5. Enter the password.

NOTE

If you have forgotten password, you can click the **Forgot Password** and reset your password. The Forgot Password link resets only your Aruba Central account; hence, it is not available to SSO users.

6. If you have forgotten your password,
7. Click **Continue**. The **Initial Setup** wizard opens.

- If you have a paid subscription, click **Get Started** and set up your account.
- If you are a trial user, click **Evaluate Now** and start your trial.

Changing Your Password

To change your Aruba Central account:

1. In the Aruba Central UI, click the user icon (👤) in the header pane.
2. Click **Change Password**.

3. Enter a new password.
4. Log in to Aruba Central using the new password.

NOTE

The **Change Password** menu option is not available for federated users who sign in to Aruba Central using their SSO credentials.

Logging Out of Aruba Central

To log out of Aruba Central:

1. In the Aruba Central UI, click the user icon (👤) in the header pane.
2. Click **Logout**.

Was this information helpful? 👍 Yes 👎 No

Explore Aruba Central

Visit our website and sign up for Aruba Central today!

Contact Us

Site Feedback
Support Case
HPE Support Center

Ask the Community

Join the discussion in the Aruba AirHeads community

REFERENCE 5

HPE GreenLake

HPE GreenLake Developer Portal Guides Services Community About HPE GreenLake Login

Last updated 2024-12-02T20:01:46.000Z

HPE GreenLake platform API and Events catalog

HPE GreenLake platform provides an extensive catalog of APIs and Events. By providing both API and Event functionality, HPE GreenLake offers a comprehensive developer toolkit that meets the diverse needs and use cases of HPE GreenLake administrators.

HPE GreenLake APIs allow you to request and retrieve data on demand, initiating and executing operations programmatically, granting access to the functionalities available through the HPE GreenLake platform UI. You can manage devices and subscriptions through these APIs, view audit logs, and perform various other tasks.

HPE GreenLake platform APIs:

- Conform to the OpenAPI 3.0 specification.
- Use a single endpoint.
- Use a single OAuth token to access all APIs.
- Are built to be secure and highly available.
- Are RESTful for flexible implementation.

With HPE GreenLake Events, you can receive close to real-time notifications when specific actions or changes happen within your HPE GreenLake infrastructure.

ⓘ **GETTING HELP FROM THE HPE DEVELOPER COMMUNITY**

The HPE Developer Community provides resources like community events, blogs, and hands-on labs to help you get started and make the most out of HPE GreenLake APIs.

- Community Overview gives quick access to all sections of the HPE Developer Community.
- Community Resources curates getting started events, blogs, and labs for HPE GreenLake APIs.

API catalog

Browse the HPE GreenLake platform API catalog.

Service	Description
API Client Credentials	HPE GreenLake for API Client Credentials allows programmatic access to manage workspace credentials. You can create, delete, update, and check workspace credentials.
Audit Logs	The HPE GreenLake for Audit Log service offers a collection of RESTful APIs for publishing audit logs, managing configurations, and retrieving application-specific and overall platform logs.
Backup and Recovery	HPE GreenLake for Backup and Recovery is a data protection service that is part of the Data Services Cloud Console application on the HPE GreenLake platform.
Compute Ops	HPE Compute Ops Management offers a RESTful API to customers who want to manage their devices programmatically or through a command-line. The API enables customers to initiate any operation or task that is available through the UI web interface.
Data Services	HPE GreenLake for Data Services offers a RESTful API for capabilities common to the following APIs: Backup Recovery, Public Cloud Business Edition and Virtualization.
Devices	With the HPE GreenLake for Device Management API, you can view, manage, and onboard devices in your workspace. The API allows you to initiate any operation or task that is available through the HPE GreenLake edge-to-cloud platform UI.
Locations	HPE GreenLake for Locations is a collection of RESTful APIs for creating and managing location services. The APIs initiate any Locations service operation or task available through the HPE GreenLake platform UI. HPE GreenLake platform uses the collected information to automate service delivery and to create automated support cases.
Private Cloud Business Edition	HPE GreenLake for Private Cloud Business Edition provides global lifecycle management of infrastructure and virtualization resources.
Reporting	HPE GreenLake for Reporting provides access to reports on your HPE GreenLake platform workspace in an efficient and programmatic way.
Service Catalog	The HPE GreenLake for Service Catalog service offers a collection of RESTful APIs to fetch, provision service managers and to delete a service manager provisioned in a workspace.
Subscriptions	With the HPE GreenLake for Subscriptions APIs, you can onboard and manage subscriptions in your workspace.
Sustainability Insight Center	HPE Sustainability Insight Center APIs allow developers to access HPE Sustainability Insight Center features and data programmatically. With these APIs, you can get the total energy consumption across your IT infrastructure, information about greenhouse gas emissions, and costs associated with your energy consumption.

Service	Description
Tags	With the HPE GreenLake for Tags APIs, you can view and filter all tags and all supported tagged resources in a workspace.
User Management	HPE GreenLake for User Management API allows programmatic methods to invite or delete users and to check user information.
Virtualization	The HPE GreenLake for Virtualization API provides management of virtual machines and other virtual resources in public clouds and on-premises systems.
Wellness	The HPE GreenLake for Wellness APIs allow programmatic access to view and manage wellness events and insights. The APIs facilitate integrating wellness events into existing workflows.
Workspaces	The HPE GreenLake for Workspace Management APIs allow programmatic access to the records of workspaces and workspace-user relationships.

Event catalog

Browse the HPE GreenLake platform Events catalog. To learn more about HPE GreenLake platform Events, see Events.

Service	Description
Audit Logs	The HPE GreenLake for Audit Log service provides an event that notifies when an audit log has been created.
Expiring Subscriptions	The HPE GreenLake for Expiring subscriptions that notifies when a Subscription is expiring in 1, 30, 60 and 90 days.

Privacy Terms of Use Ad Choices & Cookies Do Not Sell or Share My Personal Ir

REFERENCE 6

You are here: Home > Aruba Central Overview > Getting Started > Exploring the User Interface

About the Aruba Central App User Interface

The Aruba Central helps you to manage, monitor, and analyze your network.

This topic discusses the following:

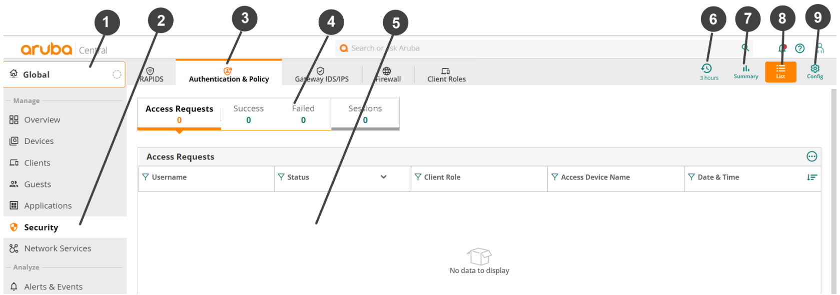
- Types of Dashboards in the Aruba Central app
- Navigating to the Switch, Access Point, or Gateway Dashboard
- Workflow to Configure, Monitor, or Troubleshoot in the Aruba Central app

Aruba offers the following variants of the **Aruba Central** app user interface:

- **Standard Enterprise mode**— This mode is intended for customers who manage their respective accounts end-to- end. In the Standard Enterprise mode, the customers have complete access to their accounts. They can also provision and manage their respective accounts.
- **Managed Service Provider (MSP) mode**— This mode is for managed service providers who need to manage multiple customer networks. With MSP mode enabled, the MSP administrators can provision customer accounts, allocate licenses, assign licenses, and monitor customer accounts and their networks. The administrators can also drill down to a specific tenant account and perform administration and configuration tasks. The tenants can access only their respective accounts, and only those features and application services to which they have subscribed.

The following image displays the navigational elements of the **Aruba Central** app in the Standard Enterprise mode. However, the navigational elements also apply to the MSP mode.

Figure 1 *Navigation Elements of the **Aruba Central** app*



Callout Number	Description
1	Filter to select an option under **Groups**, **Labels**, or **Sites**. For all devices, select **Global**. A corresponding dashboard is displayed.
2	Item under the left navigation contextual menu. The menu is dependent on the filter selection.
3	First-level tab on the dashboard.
4	Second-level tab on the dashboard.
5	Dashboard content for the selected view and filter. For example, the current dashboard in the image displays the **UCC** tab under **Manage** > **Applications** in the **List** view for the **Global** filter.
6	Time range filter. This is displayed for selected dashboards only.
7	**List** view to display tabular data for the selected filter. This is displayed for selected dashboards only.
8	**Summary** view to display charts for the selected filter. This is displayed for selected dashboards only.
9	**Config** view to enable configuration options for the selected filter. This is displayed for selected dashboards only.

Types of Dashboards in the Aruba Central app

The **Aruba Central** app uses a filter to set the dashboard context for the app. The menu for the left navigation pane changes according to the selected filter value. Selecting any item on the left navigation pane displays a corresponding dashboard. Accordingly, for different values of the filter, the content displayed for the left navigation menu and the dashboard context differs. The following table lists down all the available dashboards and the link to the detailed description of each type of dashboard.

Table 1: *Types of Dashboards*

Link to the Dashboard	Filter Value and Dashboard Description
The Global Dashboard	When the filter is set to **Global** (for standard enterprise modes) or **All Groups** (for managed service modes), the dashboard context displayed is for all available devices registered to the specific Aruba Central account. This is called the global dashboard.

	devices that are configured as part of that site. This is called the site dashboard.
The Label Dashboard	When the filter is set to a specific label, the dashboard context displayed is only for the devices that are configured as part of that label. This is called the label dashboard.
The Gateway Dashboard	When the filter is set to a gateway, the dashboard context displayed is only for the that specific gateway. This is called the gateway dashboard. The gateway dashboard enables you to manage and monitor a specific gateway.
The Access Point Dashboard	When the filter is set to an access point, the dashboard context displayed is only for the that specific access point. This is called the access point dashboard. The access point dashboard enables you to manage and monitor a specific access point.
The Switch Dashboard	When the filter is set to a switch, the dashboard context displayed is only for the that specific switch. This is called the switch dashboard. The switch dashboard enables you to manage and monitor a specific switch.
The Client Dashboard	In the **Aruba Central** app, the client dashboard is displayed under **Manage** > **Clients** for any filter value.

The dashboard for any item on the left navigation menu can have a combination of the following views:

- **Summary** view— Click the Summary **Summary** icon to display the summary dashboard. The summary dashboard displays a number of charts. For example, for the global dashboard, under **Manage**, the **Overview** > **Network Health** tab in **Summary** view displays a map of the available sites and their corresponding health. If available, use the time range filter to change the time-lines for the charts.
- **List** view— Click the List **List** icon to display tabular data for a selected dashboard. For example, for the global dashboard under **Manage**, the **Overview** > **Network Health** tab in **List** view displays a list of the available sites managed by Aruba Central. If available, use the time range filter to change the time-lines for the tabular data.
- **Config** view— Click the Config **Config** icon to enable the configuration options for a specific dashboard. For example, for the global dashboard under **Manage**, the **Applications** > **UCC** tab in **Config** view displays various configuration options for UCC.
- **AOS-CX** view— Click the AOS-CX **AOS-CX** icon to enable the configuration options for AOS-CX switches.
- **AOS-S** view— Click the AOS-S **AOS-S** icon to enable the configuration options for the AOS-S switches.

The **Summary**, **List**, and **Config** icons are displayed in the same order for all dashboards. The default view is displayed when you select any item on the left navigation menu and the tabs on the dashboard. For example, if you select the **Global** filter, and then select **Devices** on the left navigation menu, the **List** view is displayed for all the tabs on the dashboard by default. If you select **Overview** on the left navigation menu, the **Summary** view is displayed by default.

On any dashboard, when you select a view, the view is retained when you switch between the tabs on the same dashboard. If a particular view is not applicable for a tab, the default view for the tab is selected. For example, if you select the **Global** filter, and then select **Manage** > **Devices** > **Access Points**, the **List** view is displayed by default. When you are in the **Access Points** tab, if you select the **Summary** view, and then select the **Switches** tab, the **Summary** view for the **Switches** tab is displayed.

Navigating to the Switch, Access Point, or Gateway Dashboard

In the **Aruba Central** app, you can navigate to a device dashboard for a switch, access point, or gateway. The device dashboard enables you to monitor, troubleshoot, or configure a single device. In order to do this, complete the following steps:

1. In the **Aruba Central** app, set the filter to a group, label, or site. For all devices, set the filter to **Global**.

   The dashboard context for the selected filter is displayed.
2. Under **Manage** > **Devices**, select one of the following options:
   - To view an access point dashboard, click the **Access Points** tab.
   - To view a switch dashboard, click the **Switches** tab.
   - To view a gateway dashboard, click the **Gateways** tab.

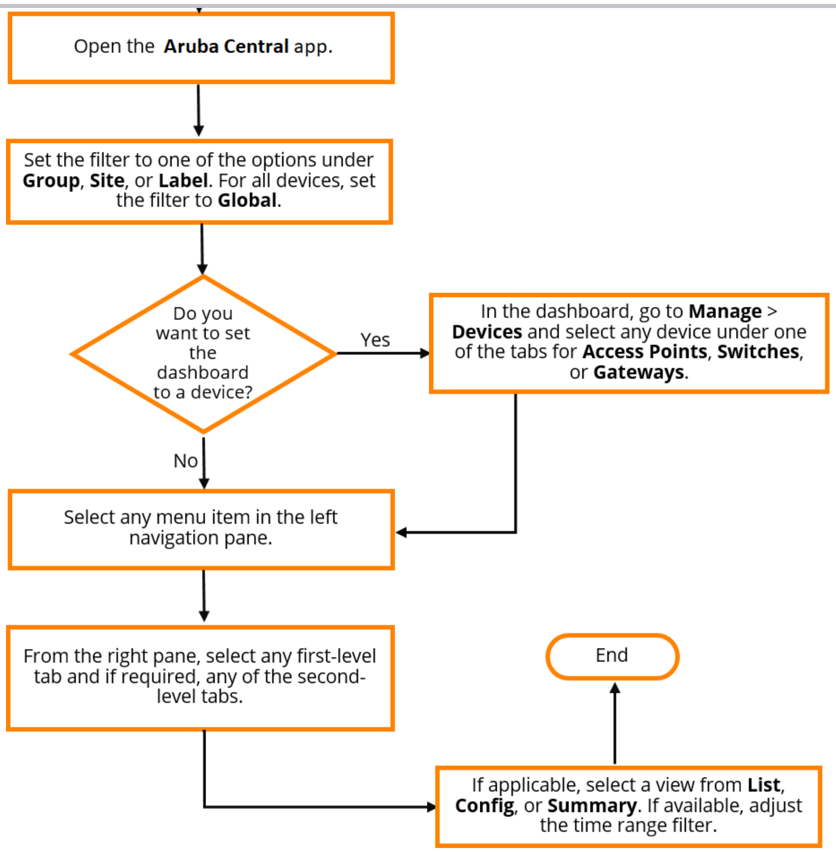
     The list of devices is displayed in **List** view.
3. Click a device listed under **Device Name**.

   The dashboard context for the specific device is displayed.

   To exit the device dashboard, click the back arrow on the filter.

Workflow to Configure, Monitor, or Troubleshoot in the Aruba Central app

The following image displays a flowchart to help you navigate the **Aruba Central** app to complete any task.


Open the **Aruba Central** app.
Set the filter to one of the options under **Group**, **Site**, or **Label**. For all devices, set the filter to **Global**.
Do you want to set the dashboard to a device?
Yes
In the dashboard, go to **Manage** > **Devices** and select any device under one of the tabs for **Access Points**, **Switches**, or **Gateways**.
No
Select any menu item in the left navigation pane.
From the right pane, select any first-level tab and if required, any of the second-level tabs.
End
If applicable, select a view from **List**, **Config**, or **Summary**. If available, adjust the time range filter.

Related Topics:

- The Standard Enterprise Mode
- About the Managed Service Portal User Interface

REFERENCE 7

AOS 10.x Terminology

Before getting started with configuring AOS 10.x, it is important to understand some important configuration concepts and terminology. The following topics are discussed in this section:

- **SSIDs**—Wireless networks are identified using a service set identifier (SSID). The SSIDs distinguish a wireless network from other networks configured within a WLAN boundary. Aruba uses the SSIDs of APs to orchestrate and configure a number of management policies.

  For more information, see WLAN SSIDs on APs.
- **Traffic Forwarding Modes**—Depending on the type of WLAN setup, the SSIDs are also used to specify the traffic forwarding modes. AOS 10.x supports automated workflows to set up these SSID profiles.

  For more information, see Traffic Forwarding Modes.
- **Supported Authentication Methods**—In creating the SSID profiles in the automated workflows, you must specify an authentication method. AOS 10.x supports a number of authentication methods and each is recommended for a specific deployment type.

  For more information, see Authentication Methods.
- **Supported Encryption Methods**—In creating the SSID profiles in the automated workflows, you must specify an encryption method. AOS 10.x supports a number of encryption methods and each is recommended for a specific deployment type.

  For more information, see Encryption Methods.
- **Cloud-Assisted Roaming Services**—The Cloud-Assisted Roaming Services feature facilitates fast roaming of 802.11r and Opportunistic Key Caching (OKC) clients, to enable seamless roaming with minimal or no disruption to the application traffic such as voice and video.

  For more information, see Cloud-Assisted Roaming Services.
- **Access Rules and Firewall Policies**—The Access Control List (ACL) is a logic that handles stateless inspection of traffic. An ACL is used in many types of implementations including routing policies and user policies. A firewall is a device that performs stateful inspection of traffic (checks for encapsulation) passing through a part of the network and decides whether to allow or deny the traffic. You can configure both ACLs and firewall policies on APs and Gateways.

  For more information, see Access Rules and Firewall Policies.
- **User Roles and VLANs**—A client connecting to a WLAN SSID that is broadcast by an AP is assigned a user role or VLAN to define the client's network privileges, the frequency of re-authentication, and the applicable bandwidth contracts.

  For more information, see User Roles and VLANs.
- **Supported Device Configuration Methods in Aruba Central**—In order to configure the management layer, Aruba Central supports a number of configuration options that includes UI workflows, templates, and APIs.

  For more information, see Device Configuration Methods in Aruba Central.

WLAN SSIDs on APs

An SSID profile on access points (APs) allows administrators to define the following elements:

- Type of WLAN and its intended users; for example, employee, guest, or voice WLAN.
- IP address assignment criteria to clients; for example, the method of assigning IP address to the clients that connect to a WLAN.
- Forwarding modes for managing client traffic.
- Security profiles for authentication of clients and encryption of client traffic.
- Firewall policies and user roles for user access control.

Traffic Forwarding Modes

AOS 10.x APs support the following deployments based on the infrastructure layer components and how traffic is managed:

- **Bridge mode**—For LAN setups, the user traffic can either be bridged locally or tunneled to a Gateway cluster for redundancy and failover. Accordingly, if the traffic is bridged locally, the infrastructure layer requires only APs. To configure AOS 10.x APs for such a deployment, you must configure the SSID in **Bridge mode**. In the **Bridge mode**, APs function as bridges between the wireless interface and the wired network deployed at a site. For example, a wireless laptop can use a bridge-mode SSID to discover network printers within the same VLAN. In the bridge mode, clients can obtain IP addresses from an external DHCP server based on the SSID specification. For more information on configuring AOS 10.x APs in a LAN setup in **Bridge mode**, see Bridge Mode Deployment.
- **Tunnel mode**—For LAN setups, where user traffic is tunneled to a gateway cluster, the infrastructure layer requires at least one Gateway in additions to the APs. A Gateway cluster is automatically formed for such AOS 10.x deployments and the cluster functions as a tunnel endpoint. To configure AOS 10.x APs for such a deployment, you must configure the SSID in **Tunnel mode**.

  In the **Tunnel mode**, APs set up a secure mobility tunnel for clients that roam between the VLANs. The client traffic is encapsulated and routed to a tunnel endpoint. The tunnel-mode SSID allows a client device to maintain a consistent IP address and experience uninterrupted access when roaming across VLANs.

  AOS 10.x employs the Decrypt-Tunnel-Mode or the D-tunnel decrypt mode in which the traffic between the AP and the Gateway is encrypted and then decrypted at the AP level. Hence, the AP performs encryption and decryption in addition to being a bridge between the clients and the Gateways.

  For more information on configuring AOS 10.x APs in a LAN setup in Tunnel mode, see Tunnel Mode Deployment.
- **Mixed mode**—Apart from **Bridge mode** and **Tunnel mode**, in specific deployments some user VLANs are on an AP uplink, while the other user VLANs are on Gateway clusters.

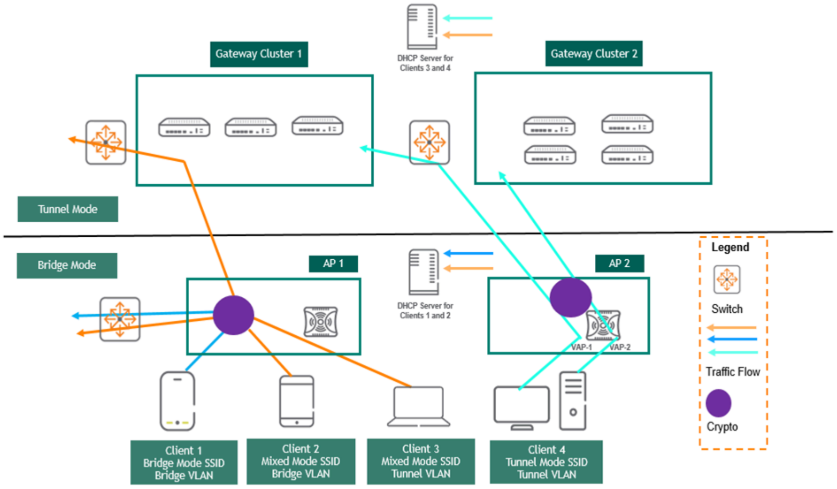
Gateway is encrypted and then decrypted at the AP level. Hence, the AP performs encryption and decryption in addition to being a bridge between the clients and the Gateways.

For more information on configuring AOS 10.x APs in a WAN setup in mixed mode, see Tunnel Mode Deployment.

- **Micro Branch mode**—For WAN setups, traffic is bridged through IPsec tunnels to a Gateway cluster. At the remote location, the infrastructure layer requires a minimum of one AP. To configure such a deployment, you must configure AOS 10.x APs in **Micro Branch mode**. For more information, see Microbranch Deployment.

The following figure illustrates the SSIDs with **Bridge**, **Tunnel**, and **Mixed** traffic forwarding modes:

Figure 1 *SSID Configuration*


Gateway Cluster 1
DHCP Server for Clients 3 and 4
Gateway Cluster 2
Tunnel Mode
Bridge Mode
AP 1
DHCP Server for Clients 1 and 2
AP 2
VAP-1
VAP-2
Legend
Switch
Traffic Flow
Crypto
Client 1 Bridge Mode SSID Bridge VLAN
Client 2 Mixed Mode SSID Bridge VLAN
Client 3 Mixed Mode SSID Tunnel VLAN
Client 4 Tunnel Mode SSID Tunnel VLAN

The above figure shows three SSIDs (in blue, orange, and green) with a client connected to each of these SSIDs. These SSIDs represent different SSID configuration and traffic forwarding modes:

- Blue—The blue line represents an SSID in the bridge forwarding mode. As illustrated in the above figure, the client traffic is bridged locally in this SSID and security policies including firewall, QoS, bandwidth contract are applied to the client traffic by the AP. Each AP acts as an authenticator with the AP IP address configured as a Network Access Server (NAS) IP in the RADIUS authentication server profiles.
- Orange—The orange line represents an SSID with the mixed forwarding mode. This SSID requires a deployment topology with a Gateway cluster in addition to the APs. The above figure shows Client 2 connected to bridge mode SSID and client 3 connected to tunnel mode SSID to illustrate that both bridge mode and tunnel mode clients can co-exist in the same SSID. Based on the VLANs to which the client is assigned, the client traffic is bridged locally or forwarded to Gateway through a secure tunnel. The AP acts as an authenticator and also applies firewall policies on the tunneled traffic.

  In the mixed forwarding mode, Captive Portal can be configured on the AP, while QoS, Firewall, Bandwidth Contract, and WAN policies can be applied on Gateway. In mixed mode, both bridged and tunneled users are authenticated through the AP. The Gateway IP address is configured as the NAS IP even for bridged users.
- Green—The green line represents an SSID with the tunnel forwarding mode. This SSID requires a deployment topology with a Gateway cluster in addition to the APs. As shown in the above figure, the client traffic is tunneled to the Gateway through different virtual APs. The Gateway receives 802.3 packets already decrypted by the AP. The AP acts an authenticator while the Gateway acts as authentication proxy. The MultiZone feature segregates the tunnel traffic of VAP-1 and VAP-2 and forwards the traffic to different Gateways under Gateway Cluster 1 and Gateway Cluster 2.

Authentication Methods

When configuring a WLAN SSIDs on APs, you can configure a number of supported authentication types for WLAN clients. These authentication methods can be configured for all traffic modes and are described in the following section:

- **802.1X Authentication**— 802.1X authentication method authenticates the identity of a user before providing network access to the user. APs support external RADIUS servers for 802.1X authentication. For authentication purpose, the wireless client can associate to a NAS or RADIUS client. NAS acts as a gateway to guard access to a protected resource. A client connecting to a SSID connects to the NAS first; therefore, based on the SSID specification, the APs or the Gateways can be configured as NAS clients to a RADIUS server to provide secure access to WLAN clients.
- **MAC Authentication**—MAC authentication is used for authenticating devices based on their physical MAC addresses. MAC authentication requires that the MAC address of a machine matches a manually defined list of addresses. This authentication method is not recommended for scalable networks and the networks that require stringent security settings. However, MAC authentication can be combined with other forms of authentication such as WEP authentication or 802.1X authentication for additional security.
- **MAC Authentication with 802.1X Authentication**—The administrators can enable MAC authentication for 802.1X authentication. If a wireless or wired client connects to the network, MAC authentication is performed first. After a successful MAC authentication is successful, 802.1X authentication is attempted. If 802.1X authentication is successful, the client is assigned an 802.1X authentication role. If 802.1X authentication fails, the client is assigned a **deny-all** role or **mac-auth-only** role.
- **Captive Portal Authentication**—Captive portal authentication is used for authenticating guest users. If the captive portal authentication profile is configured on an SSID and the guest users connect to this SSID for the Internet access, a web page with the usage policy and terms is presented to the guest users before providing access to the network. The SSID administrators can also enable authentication of guest users using an external server on cloud or outside the WLAN domain.
- **Walled Garden**—When captive portal authentication is configured on an SSID, the administrators can configure Walled garden access to allow clients to view websites in a specific domain without connecting to the Internet. For example, in a hotel

to the captive portal login page.

Encryption Methods

Aruba APs support SSIDs with the following types of encryption:

- **WPA-Enterprise and WPA-Personal**—WLAN SSIDs support security profiles with WPA for enterprise or the personal network users. WPA supports TKIP (Temporal Key Integrity Protocol), which supports a unique encryption key for each wireless frame to provide a secure connection.
- **WPA2-Enterprise and WPA-Personal**—The WPA2-Enterprise encryption uses authentication standards such as 802.1X along with other WPA2 features such as AES. WPA2-Enterprise encryption provides a secure wireless network for enterprise use. For personal wireless network, the WPA-Personal encryption type can be used along with a pre-shared key.
- **WPA3-Enterprise and WPA3-Personal**—The WPA3 encryption provides robust protection with unique encryption per user session and thus allows the SSID administrators to provide a highly secured connection even on a public Wi-Fi hotspot. WPA3-Enterprise encryption can be used to provide secure wireless network for enterprise, whereas the WPA-Personal encryption with a pre-shared key can be configured for a personal network.
- **Dynamic WEP**—Dynamic WEP encryption method combines of 802.1X authentication standard and the Extensible Authentication Protocol (EAP). With Dynamic WEP security, WEP keys are changed dynamically.
- **MPSK-AES**—Multi-Pre-Shared Key (MPSK) supports multiple PSKs simultaneously on a single SSID. MPSK-AES is supported only when Aruba ClearPass Policy Manager is configured as an authentication server on the WLAN SSID.
- **MPSK-Local**—MPSK Local supports 24 pre-shared keys per SSID without an external policy engine like ClearPass Policy Manager.

Cloud-Assisted Roaming Services

The Cloud-Assisted Roaming Services feature supports 802.11r fast transition and Opportunistic Key Caching (OKC), to enable seamless roaming with minimal or no disruption to the application traffic such as voice and video. When a client roams from one access point (AP) to another, Cloud-Assisted Roaming Services ensures that the client's wireless connection is seamless without a need for re-authentication. This feature is dependent on AirMatch to obtain the AP RF neighborhood information. It maintains a table of client key records which is updated by APs, and is propagated to neighboring APs.

The Cloud-Assisted Roaming Services feature provides seamless roaming in the following two scenarios:

- In the OKC based roaming, the AP stores one Pairwise Master Key (PMK) per client, which is derived from last 802.1x authentication completed by the client in the network. The cached PMK is used when a client roams to a new AP. This allows faster roaming of clients between the APs in a cluster, without requiring a complete 802.1X authentication.
- In case of 802.11r clients, the Cloud-Assisted Roaming Services feature is used for secure distribution of PMK-R1 to neighboring APs in Bridge-mode APs, and D-Tunnel modes where the AP acts as authenticator.

The Cloud-Assisted Roaming Services feature is enabled automatically. However, you must connect 802.11r client to 802.11r enabled SSID and OKC client to OKC enabled SSID. You can enable 802.11r and OKC in the following opmodes in the WebUI:

- WPA2-AES (802.1x), WPA2-PSK-AES (PSK), and MPSK-AES (PPSK) for 802.11r
- WPA2-AES (802.1x) for OKC

For more information on enabling the 802.11r and OKC clients in the SSID profile, see Configuring Security for a WLAN SSID Profile in Bridge Mode.

Access Rules and Firewall Policies

Aruba access points (APs) and Gateways support identity-based controls to enforce application-layer security, traffic prioritization and forwarding, and network performance policies for WLAN and WAN clients.

You can configure firewall policies on the AP or Gateway cluster to define user access to network, set a priority queue for Quality of Service (QoS), and assign bandwidth contracts.

A firewall policy identifies specific characteristics about a data packet and performs one of the following actions:

- Firewall action such as permitting or denying the packets.
- Administrative action such as logging the packets.
- The QoS action such as placing packets in a priority queue.

You can configure the following types of ACLs on APs and Gateways.

- **Standard ACL**—Permits or denies traffic based on the source IP address of the packet. Standard ACLs use a bit-wise mask to specify the portion of the source IP address to be matched.
- **Extended ACLs**—Permits or denies traffic based on source or destination IP address, source or destination port number, or IP protocol.
- **MAC ACLs**—Filters traffic on a specific source MAC address or range of MAC addresses.
- **Ethertype ACLs**—Filters traffic based on the Ethertype field in the frame header. Ethertype ACLs can be used to permit IPs while blocking other non-IP protocols, such as IPX or AppleTalk.
- **Session ACLs**—Restricts all services from specific hosts and subnets. Rules with this ACL are applied to all traffic on the AP or Gateway regardless of the ingress port or VLAN.
- **Route ACLs**—Forwards all packets to a device defined by an IPsec map, a next hop list, a tunnel or a tunnel group.

User Roles and VLANs

A client connecting to a WLAN SSID that is broadcast by an access point (AP) is assigned a user role to define the client's netw privileges, the frequency of re-authentication, and the applicable bandwidth contracts.

A client device is assigned a user role by several methods:

- Initial user role—The initial user role or VLAN assigned for the unauthenticated clients.
- User-derived role—The user role can be derived from user attributes when a client connects to an AP. You can configure access rules for a user role and assign it to the clients when they match the criteria defined in the user role. For example, you

authenticates to an authentication server, the user role for the client can be based on one or more attributes returned by the server during authentication. Server-derived roles are assigned after clients complete the authentication.

- VSA-Derived Role—Many NAS vendors, including Aruba, use vendor-specific attributes to provide features that are not supported in standard RADIUS attributes. The Aruba VSAs allow deriving user roles and VLAN for the clients that authenticate to the RADIUS server. A role derived from a VSA takes precedence over other types of user roles.

Device Configuration Methods in Aruba Central

Aruba Central offers the following options for configuring devices in your account:

- **Groups**—You can use the Groups feature to create a logical subset of devices. If you have devices that must share common configuration settings, ensure that you assign these devices to the same group. Any new device joining a group inherits the configuration that is already applied on the devices in a group.
- **Device-specific configuration**—If you have fewer devices that do not have the same configuration requirements, you can apply configuration changes at the device level. In some cases, although the devices are assigned to a group, you may want to have a slightly different configuration on one specific device in a group. In such cases, you can modify the device configuration and apply changes at the device level.
- **Configuration templates**—You can also leverage the configuration templates feature to quickly deploy. To use a template-based configuration method for APs, ensure that you enable the template-based configuration mode when creating AP groups.

REFERENCE 8

Legal Disclaimer: The resource assets in this website may include abbreviated and/or legacy terminology for HPE Aruba Networking products. See www.arubanetworks.com for current and complete HPE Aruba Networking product lines and names.

Search

You are here: Home > Configuring Access Points in HPE Aruba Networking Central

Configuring Access Points in HPE Aruba Networking Central

HPE Aruba Networking Central allows you to configure various AP properties such as WLAN SSID profiles, radio profiles, authentication and security parameters, along with system parameters in both Instant APs and HPE Aruba Networking Wireless Operating System 10 APs.

Refer to the following topics for more information:

- Configuring Instant APs in HPE Aruba Networking Central
- Configuring AOS-10 APs in HPE Aruba Networking Central
- Microbranch Deployment

Configuring Instant APs in HPE Aruba Networking Central

Configuring AOS-10 APs in HPE Aruba Networking Central

Microbranch Deployment

| Product Documentation
Release Notes ▼
PDFs
Support
More ▼

Configuring Instant APs in HPE Aruba Networking Central

Configuring AOS-10 APs in HPE Aruba Networking Central

Microbranch Deployment

REFERENCE 9

Search

You are here: Home > Aruba Instant User Guide > Table of Contents > Automatic Retrieval of Configuration

Automatic Retrieval of Configuration

This chapter provides the following information:

Managed Mode Operations

Instant APs support managed mode operations to retrieve the configuration file from a server through the FTP or FTPS, and automatically update the Instant AP configuration.

The server details for retrieving configuration files are stored in the basic configuration of the Instant APs. The basic configuration of an Instant AP includes settings specific to an Instant AP, for example, host name, static IP, and radio configuration settings. When an Instant AP boots up, it performs a GET operation to retrieve the configuration (.cfg) file from the associated server using the specified download method.

After the initial configuration is applied to the Instant APs, the configuration can be changed at any point. You can configure a polling mechanism to fetch the latest configuration by using an FTP or FTPS client periodically. If the remote configuration is different from the one running on the Instant AP and if a difference in the configuration file is detected by the Instant AP, the new configuration is applied. At any given time, Instant APs can fetch only one configuration file, which may include the configuration details specific to an Instant AP. For configuring polling mechanism and downloading configuration files, the users are required to provide credentials (username and password). However, if automatic mode is enabled, the user credentials required to fetch the configuration file are automatically generated. To enable automatic configuration of the Instant APs, configure the managed mode command parameters.

Prerequisites

Perform the following checks before configuring the managed mode command parameters:

- Ensure that the Instant AP is running Instant 8.3.0.0 or later versions.
- When the Instant APs are in the managed mode, ensure that the Instant APs are not managed by AirWave.

Configuring Managed Mode Parameters

To enable the automatic configuration, perform the steps described in the following table:

Table 1: *Managed Mode Commands*

No.	Steps	Command
1.	Start a CLI session to configure the managed-mode profile for automatic configuration.	(Instant AP)(config)# managed-mode-profile

2.	Enable automatic configuration
	Or
	Specify the user credentials.
		`(Instant AP)(managed-mode-profile)#  automatic`
		Or
		`(Instant AP)(managed-mode-profile)# username <username>`
		`(Instant AP)(managed-mode-profile)# password <password>`
		NOTE: If the automatic mode is enabled, the user credentials are automatically generated based on Instant AP MAC address.

3.	Specify the configuration file.	`(Instant AP)(managed-mode-profile)# config-filename  <file_name>` `Filename`—Indicates filename in the alphanumeric format. Ensure that configuration file name does not exceed 40 characters.
4.	Specify the configuration file download method.	`(Instant AP)(managed-mode-profile)# download-method <ftp|ftps>` You can use either FTP or FTPS for downloading configuration files.

No.	Steps	Command
5.	Specify the name of the server or the IP address of the server from which the configuration file must be downloaded.	(Instant AP)(managed-mode-profile)# server <server_name>
6.	Configure the day and time at which the Instant APs can poll the configuration files from the server.	`(Instant AP) (managed-mode-profile)# sync-time day <dd> hour <hh> min <mm> window <window>` Based on the expected frequency of configuration changes and maintenance window, you can set the configuration synchronization timeline. ▪ `day <dd>`—Indicates day, for example to configure Sunday as the day, specify 01. To configure the synchronization period as everyday, specify 00. ▪ `hour <hh>`—Indicates hour within the range of 0–23. ▪ `min <mm>`—Indicates minutes within the range of 0–59. ▪ `window <hh>`—Defines a window for synchronization of the configuration file. The default value is 3 hours.
7.	Configure the time interval in minutes between two retries, after which Instant APs can retry downloading the configuration file.	`(Instant AP)(managed-mode-profile)# retry-poll-period <seconds>` **NOTE:** Specify the retry interval in seconds within the range of 5–60 seconds. The default retry interval is 5 seconds.

8.	Apply the configuration changes.	`(Instant AP)(managed-mode-profile)# end`
		`(Instant AP)# commit apply`

If you want to apply the configuration immediately and do not want to wait until next configuration retrieval attempt, execute the following command:

```
(Instant AP)# managed-mode-sync-server
```

Verifying the Configuration

To verify if the automatic configuration functions, perform the following checks:

1. Verify the status of configuration by running the following commands at the command prompt:

```
(Instant AP)# show managed-mode config
(Instant AP)# show managed-mode status
```

2. Verify the status of download by running the following command at the command prompt:

```
(Instant AP)# show managed-mode logs
```

If the configuration settings retrieved in the configuration file are incomplete, Instant APs reboot with the earlier configuration.

REFERENCE 10

Legal Disclaimer: The resource assets in this website may include abbreviated and/or legacy terminology for HPE Aruba Networking products. See www.arubanetworks.com for current and complete HPE Aruba Networking product lines and names.

Getting Started with HPE Aruba Networking Central

Accessing HPE Aruba Networking Central

How do I access HPE Aruba Networking Central?

- HPE Aruba Networking Central can be accessed using one of the following HPE GreenLake portal URLs:
  - https://console.greenlake.hpe.com
  - https://auth.hpe.com

How do I manage users in HPE Aruba Networking Central? What are the supported user authentication methods?

- Identity, access, and authentication are managed using the HPE GreenLake platform.

  For more information on managing users in HPE Aruba Networking Central, see the HPE GreenLake Edge-to-Cloud Platform User Guide.

- Users can authenticate by using their login credentials with an optional multi-factor authentication or federated single sign-on (SSO) using SAML 2.0.

NOTE

Users authenticated through SSO-SAML can access up to eight workspaces. Contact HPE GreenLake support, if you need access beyond the supported limit.

- HPE GreenLake supports both service provider and identity-provider initiated SSO.
- The supported identity providers for HPE GreenLake include Okta, Microsoft, and Google.

NOTE

Supported identity providers for HPE GreenLake and HPE Aruba Networking Network Access Control (NAC) products are mutually exclusive.

Initial Setup

What is a cluster zone?

A cluster zone refers to an HPE Aruba Networking Central deployment area within a specific region. In other words, cluster zones are a regional grouping of one or more container instances in which HPE Aruba Networking Central is deployed. Cluster zones allow your deployments to restrict customer data to a specific region and plan time zone-specific maintenance windows.

Table 1: *Cluster Zone URLS*

Cluster Zone	Portal URL	Application URL
US-1	https://portal.central.arubanetworks.com	https://app.central.arubanetworks.com
US-2	https://portal-prod2.central.arubanetworks.com	https://app-prod2.central.arubanetworks.com
US-WEST-4	https://portal-uswest4.central.arubanetworks.com	https://app-uswest4.central.arubanetworks.com
Canada-1	https://portal-ca.central.arubanetworks.com	https://app-ca.central.arubanetworks.com
China-1	https://portal.central.arubanetworks.com.cn	https://app.central.arubanetworks.com.cn
EU-1	https://portal-eu.central.arubanetworks.com	https://app2-eu.central.arubanetworks.com

APAC-1	https://portal-apac.central.arubanetworks.com	https://app2-ap.central.arubanetworks.com
APAC-EAST1	https://portal-apaceast.central.arubanetworks.com	https://app-apaceast.central.arubanetworks.com
APAC-SOUTH1	https://portal-apacsouth.central.arubanetworks.com	https://app-apacsouth.central.arubanetworks.com

What is a subscription key?

A subscription key is a 14-character alphanumeric string; for example, PQREWD6ADWERAS.

Subscription keys allow your devices to be managed by HPE Aruba Networking Central.

How do I add a new subscription key?

You can add a subscription key using the **Devices** option in HPE GreenLake platform.

For more information, see the **Devices** section in the HPE GreenLake Edge to Cloud Platform User Guide.

What does an evaluation subscription include?

The evaluation subscription allows you to use the following functions in HPE Aruba Networking Central:

- Device management
- Manage up to 10 Instant APs with Advanced license
- Manage up to 5 Switches in each switch family with Foundation license:
  - 6100/25xx/low density (16 ports or less)
  - 6200/29xx
  - 6300/3810
  - 8xxx/6400/5400
- Manage up to 10 HPE Aruba Networking70xx and 2 HPE Aruba Networking72xx Gateways with Advanced license
- Manage up to 5 HPE Aruba Networking90xx Gateways using Advanced with Security license
- Monitoring—Monitor your devices, network and client status
- Guest Access app—Set up guest Wi-Fi on your custom portals
- Presence Analytics—Analyze consumer presence data for your stores
- Troubleshooting—Run diagnostic checks and troubleshoot device issues

What is a subscriber ID? Where can I find it?

The subscriber ID or the customer ID is the identity number assigned to your HPE Aruba Networking Central account. To view your subscriber ID in the HPE Aruba Networking Central UI, click the user icon (👤) at the top right corner of the filter bar.

How do I find the MAC address and Serial Number of a device?

You can find the MAC address and serial number of HPE Aruba Networking devices on the front or back of the hardware.

What types of subscriptions does HPE Aruba Networking Central support?

HPE Aruba Networking Central supports the following types of licenses:

- Foundation—This license provides all the features included in the Device Management subscription and some additional features that were available as a value- added services for APs in the earlier licensing model.
- Advanced—This license provides all the features of a Foundation License, with additional features related to AI insights.

How do devices communicate with HPE Aruba Networking Central?

Most HPE Aruba Networking devices support ZTP. When you power on a device and connect it to your provisioning network, devices such as Instant APs and SD-WAN Gateways connect to the Activate server and download the provisioning parameters. If HPE Aruba Networking Central is set as the management entity, devices automatically connect to HPE Aruba Networking Central.

Devices communicate with HPE Aruba Networking Central using HTTPS WebSockets. To manage your devices from HPE Aruba Networking Central, ensure that the following firewall ports are open.

This section includes the following topics:

- Domain Names for Streaming Telemetry

- Cloud Guest Server Domains for Guest Access Service
- Domain Names for OpenFlow
- Domain Names for RCS
- Other Domain Names

Domain Names for Streaming Telemetry

Domain names to be allow listed for streaming telemetry.

Table 2: *Domain Names for Streaming Telemetry*

Region	Domain Name	Protocol
US-1	app1.hybrid.central.arubanetworks.com	HTTPS TCP port 443
US-2	hc-prod2.central.arubanetworks.com	HTTPS TCP port 443
US West	uswest4-hc.central.arubanetworks.com	HTTPS TCP port 443
US West 5	uswest5-hc.central.arubanetworks.com	HTTPS TCP port 443
EU-1	central-eu-hc.central.arubanetworks.com	HTTPS TCP port 443
EU-2	eucentral2-hc.central.arubanetworks.com	HTTPS TCP port 443
EU-3	eucentral3-hc.central.arubanetworks.com	HTTPS TCP port 443
CA Central	ca-hc.central.arubanetworks.com	HTTPS TCP port 443
CN North	china-prod-hc.central.arubanetworks.com.cn	HTTPS TCP port 443
CN-2	china2-hc.central.arubanetworks.com.cn	HTTPS TCP port 443
AP South	apac-hc.central.arubanetworks.com	HTTPS TCP port 443
AP Northeast	apaceast-hc.central.arubanetworks.com	HTTPS TCP port 443
AP-SouthEast	apacsouth-hc.central.arubanetworks.com	HTTPS TCP port 443
UAE North	uaenorth1.central.arubanetworks.com	HTTPS TCP port 443

Domain Names for Device Communication with HPE Aruba Networking Central

The HPE Aruba Networking Central URLs mentioned the following table, and the HPE GreenLake portal URL mentioned in the beginning of this chapter are for region-wise administrator (or management) access to the HPE Aruba Networking Central UI.

The URLs in the following table are not applicable to AOS-CX switches.

Table 3: *Domain Names for Device Communication with HPE Aruba Networking Central*

Region	HPE Aruba Networking Central URL	URL for Device Connectivity	Protocol	FQDNs for Overlay Route Orchestrator (ORO) and Overlay Tunnel Orchestrator (OTO) Services
US-1	app.central.arubanetworks.com	app1.central.arubanetworks.com	HTTPS TCP port 443	app1-h2.central.arubanetworks.com
US-2	app-prod2.central.arubanetworks.com	device-prod2.central.arubanetworks.com	HTTPS TCP port 443	device-prod2-h2.central.arubanetworks.com

US West	app-uswest4.central.arubanetworks.com	device-uswest4.central.arubanetworks.com	HTTPS TCP port 443	device-uswest4-h2.central.arubanetworks.com
US West 5	app-uswest5.central.arubanetworks.com	device-uswest5.central.arubanetworks.com	HTTPS TCP port 443	device-uswest5-h2.central.arubanetworks.com
EU-1	app2-eu.central.arubanetworks.com	device-eu.central.arubanetworks.com	HTTPS TCP port 443	device-eu-h2.central.arubanetworks.com
EU-2	app-eucentral2.central.arubanetworks.com	device-eucentral2.central.arubanetworks.com	HTTPS TCP port 443	device-eucentral2-h2.central.arubanetworks.com
EU-3	eucentral3.central.arubanetworks.com	device-eucentral3.central.arubanetworks.com	HTTPS TCP port 443	device-eucentral3-h2.central.arubanetworks.com
CA Central	app-ca.central.arubanetworks.com	device-ca.central.arubanetworks.com	HTTPS TCP port 443	device-ca-h2.central.arubanetworks.com
CN North	app.central.arubanetworks.com.cn	device.central.arubanetworks.com.cn	HTTPS TCP port 443	device-h2.central.arubanetworks.com.cn
CN-2	app-china2.central.arubanetworks.com.cn	device-china2.central.arubanetworks.com.cn	HTTPS TCP port 443	device-china2-h2.central.arubanetworks.com.cn
AP South	app2-ap.central.arubanetworks.com	app1-ap.central.arubanetworks.com	HTTPS TCP port 443	app1-ap-h2.central.arubanetworks.com
AP Northeast	app-apaceast.central.arubanetworks.com	device-apaceast.central.arubanetworks.com	HTTPS TCP port 443	device-apaceast-h2.central.arubanetworks.com
AP SouthEast	app-apacsouth.central.arubanetworks.com	device-apacsouth.central.arubanetworks.com	HTTPS TCP port 443	device-apacsouth-h2.central.arubanetworks.com
UAE North	app-uaenorth1.central.arubanetworks.com	device-uaenorth1.central.arubanetworks.com	HTTPS TCP port 443	device-uaenorth1-h2.central.arubanetworks.com

Domain Names for AOS-CX Device Communication with HPE Aruba Networking Central

The HPE Aruba Networking Central URLs mentioned the following table are applicable to AOS-CX switches only.

Table 4: *Domain Names for AOS-CX Device Communication with HPE Aruba Networking Central*

Region	HPE Aruba Networking Central URL	URL for Device Connectivity	Protocol
US-1	app.central.arubanetworks.com	device-prod-d2.central.arubanetworks.com	HTTPS TCP port 443
US-2	app-prod2.central.arubanetworks.com	device-central-prod2-d2.central.arubanetworks.com	HTTPS TCP port 443
US West	app-uswest4.central.arubanetworks.com	device-uswest4-d2.central.arubanetworks.com	HTTPS TCP port 443
US West 5	app-uswest5.central.arubanetworks.com	device-uswest5-d2.central.arubanetworks.com	HTTPS TCP port 443
EU-1	app2-eu.central.arubanetworks.com	device-eu.central.arubanetworks.com	HTTPS TCP port 443
EU-2	app-eucentral2.central.arubanetworks.com	device-eu.central.arubanetworks.com	HTTPS TCP port 443
EU-3	app-eucentral3.central.arubanetworks.com	device-eucentral3-d2.central.arubanetworks.com	HTTPS TCP port 443

CN North	app.central.arubanetworks.com.cn	device-china-prod-d2.central.arubanetworks.com.cn	HTTPS TCP port 443
CN-2	app-china2.central.arubanetworks.com.cn	device-china2-d2.central.arubanetworks.com.cn	HTTPS TCP port 443
AP South	app2-ap.central.arubanetworks.com	device-apac-d2.central.arubanetworks.com	HTTPS TCP port 443
AP Northeast	app-apaceast.central.arubanetworks.com	device-apaceast.central.arubanetworks.com	HTTPS TCP port 443
AP-SouthEast	app-apacsouth.central.arubanetworks.com	device-apacsouth.central.arubanetworks.com	HTTPS TCP port 443
UAE North	app-uaenorth1.central.arubanetworks.com	device-uaenorth1-d2.central.arubanetworks.com	HTTPS TCP port 443

Domain Names for Device Communication with HPE Aruba Networking Activate

Table 5: *Domain Names for Device Communication with HPE Aruba Networking Activate*

Domain Name	Protocol
device.arubanetworks.com	HTTPS TCP port 443
devices-v2.arubanetworks.com	HTTPS TCP port 443
est.arubanetworks.com *	HTTPS TCP port 443

* Required for HPE Aruba Networking 2530 switches to provision certificate using the EST server in activate.

The device.arubanetworks.com URL is not applicable for AOS-CX switches.

For the switches to establish connection with the Activate server, when a proxy server is configured on the network, the URLs in this table must be added to the list of allowed URLs on the proxy server.

Cloud Guest Server Domains for Guest Access Service

Table 6: *Domain Names for Cloud Guest Server Access*

Region	Domain Name	Protocol
US-1	naw2.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443
	naw2-elb.cloudguest.central.arubanetworks.com	TCP port 443
US-2	nae1.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443
	nae1-elb.cloudguest.central.arubanetworks.com	TCP port 443
US West	uswest4.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443
	uswest4-elb.cloudguest.central.arubanetworks.com	TCP port 443
US West 5	naw2.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443
	naw2-elb.cloudguest.central.arubanetworks.com	TCP port 443
EU-1	euw1.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443
	euw1-elb.cloudguest.central.arubanetworks.com	TCP port 443
EU-2	euw2.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443
	euw2-elb.cloudguest.central.arubanetworks.com	TCP port 443
EU-3	euw3.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443

		TCP port 443
	ca-elb.cloudguest.central.arubanetworks.com	TCP port 443
CN North	cloudguest.central.arubanetworks.com.cn	TCP port 2083 TCP port 443
	cloudguest-elb.central.arubanetworks.com.cn	TCP port 443
CN-2	naw2.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443
	naw2-elb.cloudguest-elb.central.arubanetworks.com	TCP port 443
AP South	ap1.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443
	ap1-elb.cloudguest.central.arubanetworks.com	TCP port 443
AP NorthEast	apaceast.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443
	apaceast-elb.cloudguest.central.arubanetworks.com	TCP port 443
AP SouthEast	apacsouth.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443
	apacsouth-elb.cloudguest.central.arubanetworks.com	TCP port 443
UAE North	asw1.cloudguest.central.arubanetworks.com	TCP port 2083 TCP port 443
	asw1-elb.cloudguest.central.arubanetworks.com	TCP port 443

Domain Names for OpenFlow

Table 7: *Domain Names for OpenFlow*

Region	Domain Name
US-1	https://app2-ofc.central.arubanetworks.com
US-2	https://ofc-prod2.central.arubanetworks.com
US West	https://ofc-uswest4.central.arubanetworks.com
US West 5	https://ofc-uswest5.central.arubanetworks.com
EU-1	https://app2-eu-ofc.central.arubanetworks.com
EU-2	https://ofc-eucentral2.central.arubanetworks.com
EU-3	https://ofc-eucentral3.central.arubanetworks.com
CA Central	https://ofc-ca.central.arubanetworks.com
CN North	https://ofc.central.arubanetworks.com.cn
CN-2	https://ofc-china2.central.arubanetworks.com.cn
AP South	https://app2-ap-ofc.central.arubanetworks.com
APNorthEast	https://ofc-apaceast.central.arubanetworks.com
AP SouthEast	https://ofc-apacsouth.central.arubanetworks.com
UAE North	https://ofc-uaenorth1.central.arubanetworks.com

Domain Names for RCS

Table 8: *Domain Names and URLs for RCS*

Region	Domain Name	Protocol
US-1	rcs-ng-prod.central.arubanetworks.com	SSH port 443
	rcs-ng-xp-prod.central.arubanetworks.com	
US-2	rcs-ng-central-prod2.central.arubanetworks.com	SSH port 443

	rcs-ng-xp-uswest4.central.arubanetworks.com	
US West 5	rcs-ng-uswest5.central.arubanetworks.com	SSH port 443
EU-1	rcs-ng-eu.central.arubanetworks.com	SSH port 443
	rcs-ng-xp-eu.central.arubanetworks.com	
EU-2	rcs-ng-eucentral2.central.arubanetworks.com	SSH port 443
	rcs-ng-xp-eucentral2.central.arubanetworks.com	
EU-3	rcs-ng-eucentral3.central.arubanetworks.com	SSH port 443
	rcs-ng-xp-eucentral3.central.arubanetworks.com	
CA Central	rcs-ng-starman.central.arubanetworks.com	SSH port 443
	rcs-ng-xp-starman.central.arubanetworks.com	
CN North	rcs-ng-china-prod.central.arubanetworks.com.cn	SSH port 443
CN-2	rcs-ng-china2.central.arubanetworks.com.cn	SSH port 443
AP South	rcs-ng-apac.central.arubanetworks.com	SSH port 443
	rcs-ng-xp-apac.central.arubanetworks.com	
AP NorthEast	rcs-ng-apaceast.central.arubanetworks.com	SSH port 443
	rcs-ng-xp-apaceast.central.arubanetworks.com	
AP SouthEast	rcs-ng-apacsouth.central.arubanetworks.com	SSH port 443
	rcs-ng-xp-apacsouth.central.arubanetworks.com	
UAE North	rcs-ng-uaenorth1.central.arubanetworks.com	SSH port 443

Other Domain Names

Table 9: *Other Domain Names*

Domain Name	Protocol	Description
sso.arubanetworks.com	TCP port 443	Allows users to access their accounts on the internal server.
internal.central.arubanetworks.com internal2.central.arubanetworks.com	TCP port 443	Allows users to access the HPE Aruba Networking Central Internal portal.
pool.ntp.org	UDP port 123	Allows the device to update the internal clock and configure time zone when a factory default device comes up. By default, the HPE Aruba Networking devices contact **pool.ntp.org** and use NTP to synchronize their system clocks.
activate.arubanetworks.com	TCP port 443	Allows the device to configure provisioning rules in Activate.
stun.pqm.arubanetworks.com	UDP or TCP port 3478 and 3479	Allows the device to discover public IP over the WAN uplinks configured on devices.
pqm.arubanetworks.com	ICMP or UDP port 4500	Allows the device to check the health of WAN uplinks configured on Branch Gateways.
http://h30326.www3.hpe.com	TCP port 433	Allows users to access the HPE Aruba Networking AP software images. To view the URL for software updates, use the **show activate software-update** command.
common.cloud.hpe.com/ccssvc/ccs-system-firmware-registry	TCP port 80 and TCP port 443	Allows the device to access the CloudFront server for locating all device type software images.
https://d20kce0f6gvxjn.cloudfront.net	TCP port 443	Allows the device to access the CloudFront server while Gateway IDS/IPS is enabled in HPE Aruba Networking Central gateways. **NOTE:** This URL can be invoked only by gateways that have IDPS security enabled. The URL cannot be enabled manually.

aruba.brightcloud.com	TCP port 443	Enables devices to access the Webroot Brightcloud server for application, application categories, and website content classification.
bcap15-dualstack.brightcloud.com	TCP port 443	Allows HPE Aruba Networking devices to look up the Webroot Brightcloud server for Website categories.
api-dualstack.bcti.brightcloud.com	TCP port 443	Allows HPE Aruba Networking devices to access the IP Reputation and IP Geolocation service on the Webroot Brightcloud server.
database-dualstack.brightcloud.com	TCP port 443	Allows HPE Aruba Networking devices to download the website classification database from the Webroot Brightcloud server.

When configuring ACLs to allow traffic over a network firewall, use the domain names instead of the IP addresses. For more information on ACLs, see Firewall Policies and ACLs.
For Branch Gateways to set up IPsec tunnel with the VPN concentrators, the UDP 4500 port must be open.

How do I delete a device?

The device monitoring dashboards allow you to remove an offline device. However, you will not be able to remove a device completely from HPE Aruba Networking Central database, because the device entry remains in the **Inventory** page. The devices appearing in the **Inventory** page shows the hardware devices that belong to your account or purchase order.

For more information, see the **Managing Devices** section in the HPE GreenLake Edge to Cloud Platform User Guide.

For information on removing an offline device, see the following topics:

- Deleting an Offline Access Point from the Access Points Table
- Deleting an Offline Switch
- Deleting a Gateway

What happens to a device on HPE Aruba Networking Central when it's subscription expires ?

When the subscription assigned to a device on HPE Aruba Networking Central expires and auto-subscribe is not enabled for the device, there is a 30-day grace period from the date of expiration during which the device continues to operate within the HPE Aruba Networking Central application instance. If no new subscription is assigned to the device by the end of its grace period, the device is removed from the application instance and transferred to the **Device Inventory** in HPE GreenLake platform.

What are the required firewall settings to communicate with HPE Aruba Networking Central

For more information on the required firewall settings to communicate with HPE Aruba Networking Central, see Opening Firewall Ports for Device Communication.

Navigation

How do I view the details of an AP?

To view AP details, perform the following steps:

1. In the WebUI, set the filter to **Global** for all devices or select one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the selected option contains at least one access point.
   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
3. A list of access points is displayed in the **List** view.
4. Click an AP listed under **Device Name**.

The dashboard context for an access point is displayed. Under the **Manage** > **Overview** tab, the **Access Point Details** page is displayed.

How do I configure an AP?

1. In the WebUI, select one of the following options:
   - To select a group in the filter:
     a. Set the filter to one of the options under **Groups**. Ensure that the filter selected contains at least one active access point.
     The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices** > **Access Points**. A list of access points is displayed in the **List** view.

the List view.

   c. Click an access point listed under **Device Name**. The dashboard context for the access point is displayed.

   d. Under **Manage**, click **Device** > **Access Point**.

2. Click the **Config** icon. The tabs to configure access points are displayed.

How do I view the details of a switch?

To view the properties of the switches provisioned in UI groups, perform the following procedure:

1. In the WebUI, set the filter to **Global** for all devices or select one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the selected option contains at least one switch.
   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Switches**. A list of switches is displayed in the **List** view.
3. Click a switch listed under **Device Name**. The dashboard context for the switch is displayed.
   Under the **Manage** > **Overview** tab, the **Switch Details** page is displayed.

How do I configure a switch?

To configure a switch, perform the following steps:

1. In the WebUI, select one of the following options:
   - To select a switch group in the filter:
     a. Set the filter to a group containing at least one switch.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices** > **Switches**.
   - To select a switch in the filter:
     a. Set the filter to **Global** or a group containing at least one switch.
     b. Under **Manage**, click **Devices** > **Switches**. A list of switches is displayed in the **List** view.
     c. Click a switch under **Device Name**. The dashboard context for the switch is displayed.
     d. Under **Manage**, click **Device**. The tabs to configure the switch are displayed.
2. Click the configuration icon to edit the switch properties. Tabs to access different configuration pages are displayed.

How do I view the details of a gateway?

1. In the WebUI, set the filter to **Global** for all devices or select one of the options under **Groups**, **Labels**, or **Sites**. Ensure that the selected option contains at least one gateway.
   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Devices** > **Gateways**.A list of gateways is displayed in the **List** view.
3. Click a gateway listed under **Device Name**. The dashboard context for the gateway is displayed.
   Under the **Manage** > **Overview** tab, the **Gateway Details** page is displayed.

How do I configure a gateway?

To configure a gateway, perform the following steps:

1. In the WebUI, select one of the following options:
   - To select a gateway group in the filter:
     a. Set the filter to a group containing at least one gateway.
        The dashboard context for the group is displayed.
     b. Under **Manage**, click **Devices** > **Gateways**.
   - To select a gateway in the filter:
     a. Set the filter to **Global** or a group containing at least one gateway.
     b. Under **Manage**, click **Devices** > **Gateways**. A list of gateways is displayed in the **List** view.
     c. Click a gateway under **Device Name**. The dashboard context for the gateway is displayed.
     d. Under **Manage**, click **Device**. The tabs to configure the gateway are displayed.
2. Click the configuration icon to edit the gateway properties. Tabs to access different configuration pages are displayed.

How do I access the global dashboard?

The Global dashboard displays information about all devices, groups, sites, and labels associated with the HPE Aruba Networking Central account. To access the Global dashboard, do the following:

Network, **Client Count Per Network**, **Top APs By Usage**, **Top Clients By Usage**, **Top IAP Clusters By Usage**, **Top IAP Clusters By Clients**, and **WLAN** network details. You can change the time range for the **Summary** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

To navigate to the Summary page, complete the following steps:

1. In the WebUI, set the filter to **Global**. The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Overview** > **Summary**. The Global Summary page is displayed.

How do I view AI Insights?

To view AI Insights, perform the following steps:

1. In the WebUI, set the filter to **Global**.
   The global dashboard is displayed.
2. Under **Manage**, click **Overview** > **AI Insights** to view the dashboard.

How do I view network health?

The Network Health dashboard displays information of the network sorted by site. This dashboard displays information on network devices and WAN connectivity of individual sites. To launch the **Network Health** dashboard, complete the following procedure:

1. In the WebUI, set the filter to **Global**.
2. Under **Manage**, click **Overview > Network Health** to launch the **Network Health** dashboard.

The **Network Health** dashboard has two views, list and summary. You can toggle between them by clicking the view icons.

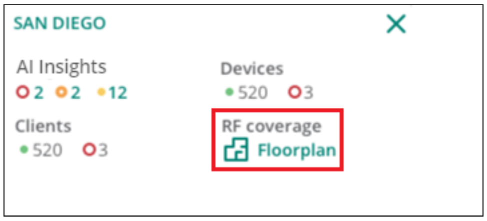
How do I access the Floor Plan dashboard?

The **Floor Plan** dashboard can be accessed from a site context or an access point context. You can either navigate to a specific site to view the floor plan or view a specific site floor plan from the **Network Health** tab in the **Global** context.

To view the **Floor Plan** dashboard from the **Network Health** tab in the **Global** context, complete the following steps:

1. In the WebUI, set the filter to **Global**.
   The global dashboard is displayed.
2. Under **Manage** > **Overview**, the **Network Health** page is displayed.
3. Hover over a site to view the following details:

   Figure 1 *Site-level Details with Floorplan Option*

   SAN DIEGO

   AI Insights
   ○2 ●2 ●12

   Devices
   ●520 ○3

   Clients
   ●520 ○3

   RF coverage
   Floorplan

4. Click **FloorPlan** under **RF Coverage**. By default, the **Floor Plan** dashboard with all floors is displayed in the summary view.
5. Click any one of the floor tiles under **All Floors** to navigate to the floor plan. To go back to the all floor tiles, click the back arrow next to the floor name.
6. To view all floors in a list, click the **Lists** view.
   A **Floor** table with a list of floors is displayed in the list view.
7. In the **Floor** table, click any one of the floors under **Name** column or enter the floor name in the **Name** column and then click the floor name to navigate to the floor plan. To go back to the floor list, click the back arrow next to the floor name.

To view the **Floor Plan** dashboard from a site context, complete the following steps:

1. In the WebUI, set the filter to one of the options under **Sites**.
   The dashboard context for the selected site is displayed.
2. Under **Manage** > **Overview**, click **Floor Plan**. By default, the **Floor Plan** dashboard with all floors is displayed in the summary view.
3. Click any one of the floor tiles under **All Floors** to navigate to the floor plan. To go back to the all floor tiles, click the back arrow next to the floor name.
4. To view all floors in a list, click the **Lists** view.
   A **Floor** table with a list of floors is displayed in the list view.

7. To go back to the floor list, click the back arrow next to the floor name.

To view the **Floor Plan** dashboard from an access point context, complete the following steps:

1. In the WebUI, set the filter to **Global**.
   The global dashboard is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.
   A list of access points is displayed in the **List** view.
3. Click the **Access Point** name to view the **Access Point Details** page. If there are many APs connected to the network, click **Online** or **Offline** to filter the online or offline APs.
4. Additionally, enter the access point name in the **Device Name** column and then click the AP name. The AP **Summary** page is displayed.
5. Under **Manage** > **Overview**, click **Floor Plan**. The floor plan details with the highlighted AP is displayed.
6. Click anywhere on the floor plan to navigate to the exact floor for a site with the AP highlighted. By default, the **Access point Details** window pops up displaying the highlighted AP details.

NOTE

The floor plan details for an AP are only accessible for the devices that are assigned with the license.

How do I view client details?

In the WebUI, you can navigate to a wired or wireless client dashboard.

1. In the WebUI, set the filter to one of the options under **Groups**, **Labels**, or **Sites**. For all devices, set the filter to **Global**.
   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Clients**. The **All Clients** page is displayed.
3. By default, the **Clients** table displays a unified list of clients for the selected group, label, site, or device.
4. Click the name of the wired or wireless client to open the corresponding dashboard for the wired or wireless client. To exit the client dashboard, click the back arrow on the filter.

How do I create a UI group?

To create a group, complete the following steps:

1. In the WebUI, set the filter to **Global**.
2. Under **Maintain**, click **Organization**. By default, the **Groups** page is displayed.
3. Click (+) **New Group**. The **Create New Group** pop-up window opens.
4. Enter a name for the group.
5. By default, HPE Aruba Networking Central enables template-based configuration method for switches and UI-workflow-based configuration method for Instant AP and Gateway.
6. To enable UI-based configuration method on all device categories:
   a. For Instant APs and Gateways, ensure that the **IAP and Gateway** check box is cleared.
   b. For switches, clear the **Switch** check box.
7. Assign a password. This password enables administrative access to the device interface.
8. Click **Add Group**.

How do I create a template group?

To create a template group, complete the following steps:

1. In the WebUI, set the filter to **Global**.
   The dashboard context for the selected filter is displayed.
2. Under **Maintain**, click **Organization**. By default, the **Groups** page is displayed.
3. Click **(+) New Group**. The **Create New Group** window is displayed.
4. Enter the name of the group.
5. Select one of the following device types for which you want to create a template group:
   - IAP and Gateway
   - Switch
6. Enter the password and confirm the password.
7. Click **Save**.

How do I view the Visibility dashboard?

The **Visibility** dashboard provides a summary of client traffic and their data usage to and from applications and websites. You can also analyze the client traffic flow using the graphs displayed in the Visibility dashboard. To view the graphs on the **Visibility** pane, ensure that the **Application Visibility** service is enabled.

To view the **Visibility** dashboard, perform the following steps:

1. In the WebUI, set the filter to one of the options under **Groups** or **Sites**. For all devices, set the filter to **Global**.
   The dashboard context for the selected filter is displayed.
2. Under **Manage**, click **Applications**. The visibility dashboard is displayed.

REFERENCE 11

Search

Configuring AOS-Switches in UI Groups

Configuring or Viewing the Switch Properties

Configuring Switch Ports on AOS-Switches

Configuring PoE Settings on AOS-Switch Ports

Configuring VLANs on AOS-Switches

Configuring Port Trunking and LACP on AOS-Switches

Enabling Spanning Tree Protocol on AOS-Switches in UI Groups

Configuring Loop Protection on AOS-Switch Ports

Configuring Port Rate Limit on AOS-Switches

Configuring RADIUS Server Settings on AOS-Switches

Configuring Downloadable

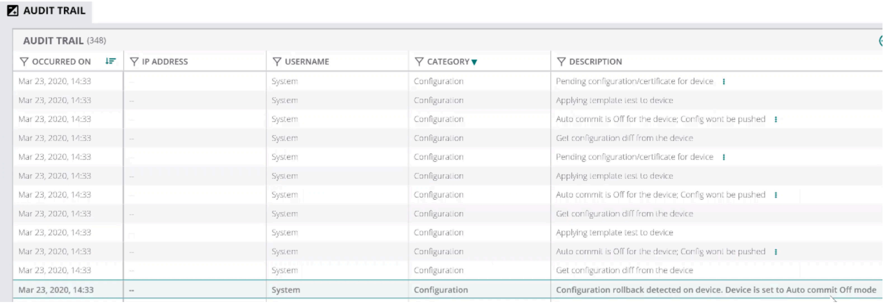
You are here: Home > Managing Switches > Configuring Aruba Switches > Automatic Rollback Configuration

Automatic Rollback Configuration

Aruba Central supports auto-rollback mechanism for AOS-Switches running software version 16.10.0009 or later. The auto-rollback mechanism is triggered when the switch loses connectivity to Aruba Central after the configuration is applied. The switch rolls back to the last known stable configuration and reconnects to Aruba Central within a period of 10 minutes. After recovery, the **Auto Commit State** in the **Configuration Audit** page is set to **Off** to stop subsequent configuration push from Aruba Central. Before changing the **Auto Commit** state to **ON**, you must review the configuration change that resulted in the network disconnect.

When a switch rollback occurs, an event will be logged in the **Audit Trail** page as shown in the following figure:

Figure 1 *Example of Audit Trail Page for Automatic Rollback Configuration*



AUDIT TRAIL

AUDIT TRAIL (348)

OCCURRED ON	IP ADDRESS	USERNAME	CATEGORY	DESCRIPTION
Mar 23, 2020, 14:33	--	System	Configuration	Pending configuration/certificate for device
Mar 23, 2020, 14:33	--	System	Configuration	Applying template test to device
Mar 23, 2020, 14:33	--	System	Configuration	Auto commit is Off for the device; Config wont be pushed
Mar 23, 2020, 14:33	--	System	Configuration	Get configuration diff from the device
Mar 23, 2020, 14:33	--	System	Configuration	Pending configuration/certificate for device
Mar 23, 2020, 14:33	--	System	Configuration	Applying template test to device
Mar 23, 2020, 14:33	--	System	Configuration	Auto commit is Off for the device; Config wont be pushed
Mar 23, 2020, 14:33	--	System	Configuration	Get configuration diff from the device
Mar 23, 2020, 14:33	--	System	Configuration	Applying template test to device
Mar 23, 2020, 14:33	--	System	Configuration	Auto commit is Off for the device; Config wont be pushed
Mar 23, 2020, 14:33	--	System	Configuration	Get configuration diff from the device
Mar 23, 2020, 14:33	--	System	Configuration	Configuration rollback detected on device. Device is set to Auto commit Off mode

REFERENCE 12

You are here: Home > Aruba Central Overview > Maintaining Aruba Central > Viewing Configuration Status

Viewing Configuration Status

Aruba Central provides an audit dashboard for reviewing configuration changes for the devices provisioned in UI and template groups. The **Configuration Audit** page is available for Instant APs, switches, and gateways.

The Configuration Audit page and the Auto Commit feature is available for Foundation and Advanced licenses for APs, switches, and gateways.

Viewing the Configuration Audit Page

To view the **Configuration Audit** page, complete the following steps:

- For Instant APs:
  a. In the **Aruba Central** app, set the filter to a group that contains at least one AP.
     The dashboard context for the selected group is displayed.
  b. Under **Manage**, click **Devices** > **Access Points**.
  c. Click the **Config** icon.
     The tabs to configure access points are displayed.
  d. Click **Show Advanced**, and click the **Configuration Audit** tab.
     The **Configuration Audit** details page is displayed.
- For Aruba switches:
  a. In the **Aruba Central** app, set the filter to a group that contains at least one switch.
     The dashboard context for the selected group is displayed.
  b. Under **Manage**, click **Devices** > **Switches**.
  c. Click the **Config** icon.
     The tabs to configure switches are displayed.
  d. Click **Configuration Audit**.
     The **Configuration Audit** details page is displayed.
- For Aruba gateways:
  a. In the **Aruba Central** app, set the filter to a group that contains at least one Branch Gateway.
     The dashboard context for the selected group is displayed.
  b. Under **Manage**, click **Devices** > **Gateways**.
  c. Click the **Config** icon.
     The tabs to configure gateways are displayed.
  d. Click **Show Advanced**, and click the **Configuration Audit** tab.
     The Configuration Audit details page is displayed.

Applying Configuration Changes

Aruba Central supports a two-staged configuration commit workflow for Instant APs and switches. Aruba Central now supports the auto commit feature at a group level. When auto commit state is enabled for a group, the configuration changes are instantly applied to all devices where auto commit state is enabled.

In the **Configuration Audit** page of the group, the **Auto Commit State** section allows administrators to switch their preference for committing configuration changes to the devices within the group.

- To enable auto commit, click **Change to Auto commit state ON**. When auto commit state is enabled for a group, the configuration changes are instantly applied to all devices where auto commit state is enabled.
- To disable auto commit, click **Change to Auto commit state OFF**. When auto commit state is disabled for a group, an administrator can build a candidate configuration, save it on cloud, review it, and then commit the configuration changes to all devices within the group.

NOTE

Aruba Central resets the auto commit state, when a device moves to another group. The device inherits the auto commit state of the group to which the device is moved.

When auto commit state is disabled for a group, Aruba Central restricts modification to the auto commit state at a device level. When auto commit state is enabled for a group, Aruba Central allows modification to the auto commit state at a device level.

The auto commit at a group level is not applicable for Aruba gateways in the **Configuration Audit** page. Auto commit state is always enabled for Aruba gateways.

Viewing and Editing

To modify the auto commit state of devices within the group, when **Auto Commit State** for a group is enabled, complete the following steps:

1. Click **View & Edit** under **Auto Commit State: ON** tile.
2. Select a device name, click **Disable Auto Commit**, and then click **OK**.

1. Click **View & Edit** under **Auto Commit State: OFF** tile.
2. Select a device name, click **Enable Auto Commit**, and then click **OK**.
3. Click **Yes** in the **Confirm Action** dialog box.

When auto commit state for a group is disabled, the **View & Edit** link is disabled to restrict modifications to the auto commit state of the devices within the group. When auto commit state for a group is enabled, the **View & Edit** link allows you to modify the auto commit state of the devices within the group.

Auto Commit Workflow

To enable Aruba Central to commit configuration changes instantly, complete the following steps:

1. In the **Aruba Central** app, set the filter to a group that contains at least one AP and a switch.

   The dashboard context for the selected group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.

   In Aruba Central, the auto commit workflow for a group can be implemented either from the switch configuration audit page or Instant AP configuration audit page. Alternatively, you can navigate to **Devices** > **Switches**.
3. Click the **Config** icon.

   The tabs to configure access points are displayed.
4. Click **Show Advanced**, and click the **Configuration Audit** tab.

   The **Configuration Audit** details page is displayed.
5. Ensure that the **Auto Commit State** for the group is set to **ON**.
6. Based on configuration mode set for the devices in the group, use either the UI workflows or a configuration template to complete the configuration workflow and save the changes. Aruba Central automatically commits the configuration changes to all devices where auto commit state is enabled.
7. View the **Local Overrides and Configuration Sync Issues**, if any.

Aruba Central does not support the two-staged configuration commit workflow for Aruba gateways.
The tenant accounts in the MSP deployments do not inherit the **Auto Commit State** configured at the MSP level. The tenant account users can enable or disable **Auto Commit** state for the devices in their respective accounts.

Manual Commit Workflow

To build configuration and review it before committing the configuration changes, complete the following steps:

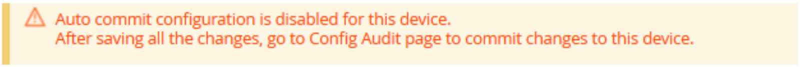
1. In the **Aruba Central** app, set the filter to a group that contains at least one AP and a switch.

   The dashboard context for the selected group is displayed.
2. Under **Manage**, click **Devices** > **Access Points**.

   In Aruba Central, the manual commit workflow for a group can be implemented either from the switch configuration audit page or Instant AP configuration audit page. Alternatively, you can navigate to **Devices** > **Switches**.
3. Click the **Config** icon.

   The tabs to configure access points are displayed.
4. Click **Show Advanced**, and click the **Configuration Audit** tab.

   The **Configuration Audit** details page is displayed.
5. Ensure that the **Auto Commit State** for the group is set to **OFF**.
6. Based on configuration mode set for the device, use either the UI workflows or a configuration template to complete the configuration workflow and save the changes. When you try to save the save changes, Aruba Central displays the following warning message:



⚠ Auto commit configuration is disabled for this device.
After saving all the changes, go to Config Audit page to commit changes to this device.

7. When the auto commit state for a group is set to **OFF**, and changes are configured to the devices at a group level, Aruba Central displays the following warning message when you try to save the changes:

9. Click **Commit Now** to commits the configuration changes to all devices within the group.

Viewing Configuration Overrides and Errors

The **Configuration Audit** page allows you to view the configuration push errors, template synchronization errors, configuration sync, and device level configuration overrides. Some of notable status indicators available on the page includes:

- **Configuration Status**—Provides details of the number of devices with configuration sync errors. To view the devices with configuration sync errors, click **View Details**. The **Config Difference** window is displayed. You can view configuration differences for each device within the group.
- **Local Overrides**—Provides details of the number of devices with local overrides. To view a complete list of overrides, click **Manage Local Overrides**. The **Local Overrides** window is displayed. You can view configuration differences for each device within the group. The overrides are grouped based on the features that are configured in the UI and are displayed as drop-down sections. For example, all overrides for IGMP are listed under a separate drop-down with the heading IGMP.

  To preserve the overrides, click **Close**. To remove the overrides, select the group name with local override, type **REMOVE** in the text box and click **OK**.
- **Configuration Conflicts**—Provides details of the number of devices with configuration conflict errors. To view a complete list of configuration conflicts, click **Manage Configuration Conflicts**. The **Configuration Conflict** window is displayed. To resolve the configuration conflicts, enable the check box against each conflict, and then click **Remove** to remove the conflict.
- **Template Errors**—Provides the details of the number of devices with template errors. To view a complete list of configuration template errors, click **View Template Errors**. The **Template Errors** window is displayed. You can view a list of templates with errors.
- **Move Failures**—Aruba Central supports moving a device from one group to another. If the move operation fails, Aruba Central logs such instances as **Move Failures**.

Viewing Configuration Status for Devices at the Group Level (Template Configuration Mode)

When you select a template group from the filter, the **Configuration Audit** page displays the following information:

Table 1: *Configuration Audit Status for a Template Group*

Data Pane Content	Description
Template Errors	Provides details of the number of devices with template errors for the selected template group. Devices deployed in the template group are provisioned using configuration templates. If there are errors in the templates or variable definitions, the configuration push to the devices fails. Aruba Central records such failed instances as template errors and displays these errors on the **Configuration Audit** page. To view a complete list of errors, click **View Template Errors**. The **Template Errors** window allows you to view and resolve the template errors issues if any.
Configuration Status	Provides details of the number of devices with configuration sync errors for the selected template group. To view the configuration sync errors, click **View Details**. The Configuration Sync Issues window is displayed with the following tabs: ▪ **Not In Sync Configuration**—Displays the configuration changes that are not synched with the switch. ▪ **Device Running Configuration**—Displays the running configuration on the switch. To resolve the configuration sync errors, click **Re-Sync Configuration**. Aruba Central will attempt to synchronize the configuration with the switch or access point again. Click **Yes** in the confirmation window. To check whether the configuration was synchronized and pushed to the switch or access point, see the **Audit Trail** page.
Configuration Backup & Restore	Allows you to create a backup of templates and variables applied to the devices in the template group. For more information, see Backing Up and Restoring Configuration Templates. ▪ **New Configuration Backup**—Allows you to create a new backup of templates and variables applied to the devices in the template group.
All Devices	The **All Devices** table provides the following device information for the selected group: ▪ **Name**—The name of the device. ▪ **Type**—The type of the device. ▪ **Auto Commit**—The status of the auto commit state for all the devices within the group. ▪ **Config Sync**—Indicator showing configuration sync errors. ▪ **Template Errors**—Indicator showing configuration template errors for the devices deployed in template groups.

Viewing Configuration Status for a Device (Template Configuration Mode)

When you select a device that is provisioned in a template group, the **Configuration Audit** page displays the following information:

Table 2: *Configuration Audit Status for Devices in Template Groups*

Data Pane Content	Description
Template Applied	Displays the template that is currently applied on the selected device.
Template Errors	Displays the number of template errors for the selected device. To view a complete list of errors, click **View Template Errors**.

	- **Not In Sync Configuration**—Displays the configuration changes that are not synched with the switch. - **Device Running Configuration**—Displays the running configuration on the switch. To resolve the configuration sync errors, click **Re-Sync Configuration**. Aruba Central will attempt to synchronize the configuration with the switch or access point again. Click **Yes** in the confirmation window. To check whether the configuration was synchronized and pushed to the switch or access point, see the **Audit Trail** page.
Config Comparison Tool	Allows you to view the difference between the current configuration (**Device Running Configuration**) and the configuration that is yet to be pushed to the device (**Attempted Configuration**). To view the running and attempted configuration changes side by side, click **View**.

Viewing Configuration Status for Devices at the Group Level (UI-based Configuration Mode)

When you select an UI group, the **Configuration Audit** page displays the following information:

Table 3: *Configuration Audit Status for a UI Group*

Data Pane Content	Description
Configuration Status	Displays the number of devices with configuration sync errors for the selected UI group. To view the configuration sync errors, click **View Details**. The Configuration Sync Issues window is displayed with the following tabs: - **Not In Sync Configuration**—Displays the configuration changes that are not synched with the switch. - **Device Running Configuration**—Displays the running configuration on the switch. To resolve the configuration sync errors, click **Re-Sync Configuration**. Aruba Central will attempt to synchronize the configuration with the switch or access point again. Click **Yes** in the confirmation window. To check whether the configuration was synchronized and pushed to the switch or access point, see the **Audit Trail** page.
Local Overrides	Displays the number of devices with local overrides. To view a complete list of overrides, click **Manage Local Overrides**. The **Local Overrides** window is displayed. The overrides are grouped based on the features that are configured in the UI and are displayed as drop-down sections. For example, all overrides for IGMP are listed under a separate drop-down with the heading IGMP. - To preserve the overrides, click **Close**. - To remove the overrides, select the group name with local override, type **REMOVE** in the text box and then click **OK**.
All Devices	The **All Devices** table provides the following device information for the selected group: - **MAC Address**—MAC address of the device. - **Name**—The name of the device. - **IP Address**—IP address of the device. - **Site**—Name of the site to which the device is assigned. - **Type**—The type of the device. - **Auto Commit**—The status of the auto commit state for all the devices within the group. - **Config Sync/Config Status**—Indicator showing configuration sync errors. - **Local Overrides**—Indicator showing configuration overrides for the devices deployed in the UI groups. **NOTE:** The **MAC Address**, **IP Address**, **Site**, and **Config Status** columns are available only for groups in which Aruba gateways are provisioned (**Manage** > **Device** > **Gateways**, click the **Config** icon. The gateway configuration page is displayed. Navigate to **Configuration Audit**).

Viewing Configuration Status for a Device (UI-based Configuration Mode)

When you select a device assigned to a UI group, the **Configuration Audit** page displays the following information:

Table 4: *Configuration Audit Status for a Device Assigned to a UI Group*

Data Pane Content	Description
Configuration Status	Displays the number of devices with configuration sync errors for the selected device. To view the configuration sync errors, click **View Details**. The Configuration Sync Issues window is displayed with the following tabs: - **Not In Sync Configuration**—Displays the configuration changes that are not synched with the switch. - **Device Running Configuration**—Displays the running configuration on the switch. To resolve the configuration sync errors, click **Re-Sync Configuration**. Aruba Central will attempt to synchronize the configuration with the switch or access point again. Click **Yes** in the confirmation window. To check whether the configuration was synchronized and pushed to the switch or access point, see the **Audit Trail** page.
Local Overrides	Displays the number of local overrides. To view a complete list of overrides, click **Manage Local Overrides**. The **Local Overrides** window is displayed. The overrides are grouped based on the features that are configured in the UI and are displayed as drop-down sections. For example, all overrides for IGMP are listed under a separate drop-down with the heading IGMP. - To preserve the overrides, click **Close**.

Backing up and Restoring Configuration Templates

Aruba Central allows you to back up configuration templates assigned to the devices deployed in a template group. The **Configuration Audit** pages for Instant AP, switch, and gateway configuration containers allow you to create and manage backed up files and restore these files when required. For more information, see Backing Up and Restoring Configuration Templates.

NOTE

If monitor mode is enabled at the device level, the selected device functions in the monitor mode. If the monitor mode is enabled at the group level, all devices in the group inherit this setting.

If a device managed by Aruba Central displays a **configuration sync issue** and persistently fails to receive configuration updates from Aruba Central, contact Aruba Central Technical Support.

REFERENCE 13

Managing Sites

The **Sites** page allows you to create sites, view the list of sites configured in your setup, and assign devices to sites. The **Sites** page includes the following functions:

Table 1: *Sites Page*

Parameter	Description
Convert Labels to Sites	Allows you to convert existing labels to sites. To convert labels, download the CSV file with the list of labels configured in your setup, add the site information, and upload the CSV file. For more information, see Creating a Site.
New Site	Allows you to create a new site.
Bulk upload	Allows you to add sites in bulk from a CSV file.

Sites Table

The sites table displays a list of sites configured. It provides the following information:

Table 2: *Sites Table*

Parameter	Description
Site Name	Name of the site.
Address	Physical address of the site.
Device Count	Number of devices assigned to a site.

The table also includes the following sorting options to reset the table view on the right:

- **All Devices**—Displays all the devices provisioned in Aruba Central.
- **Unassigned**—Displays the list of devices that are not assigned to any site.

You can also use the filter and sort icons on the **Sites** and **Address** columns to filter and sort sites respectively.

Devices Table

The devices table displays a list of devices provisioned. It provides the following information:

Table 3: *Devices Table*

Parameter	Description
Name	Name of the device.
Group	Group to which the device is assigned.
Type	Type of the device.

Creating a Site

A site refers to a physical location where a set of devices are installed; for example, campus or branch. If your devices are deployed in a campus, you could create a site with the campus name. You can use the sites to monitor devices installed on a physical location.

To create a site, complete the following steps:

1. In the **Aruba Central** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
   By default, the **Network Structure** tab is displayed.
3. Click the **Sites** tile.
   The **Manage Sites** page is displayed.
4. To add a new site, click **(+) New Site**. The **Create New Site** pop-up window opens.
5. In the **Create New Site** pop-up window, enter the following details:
   a. **Site Name**—Name of the site. The site name can be a maximum of 255 single byte characters. Special characters are allowed.
   b. **Street Address**—Address of the site.
   c. **City**—City in which the site is located.
   d. **Country**—Country in which the site is located.
   e. **State/Province**—State or province in which the site is located.

You can add multiple sites by creating and importing a CSV file with mandatory information such as the site name, address, city, state, and country details.

To import site information from a CSV file, complete the following steps:

1. In the **Aruba Central** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
   By default, the **Network Structure** tab is displayed.
3. Click the **Sites** tile.
   The **Manage Sites** page is displayed.
4. Click **(+) Bulk upload**. The **Bulk Upload** pop-up opens.
5. Download a sample file.
6. Fill the site information and save the CSV file in your local directory.

NOTE

> The CSV file for bulk upload of sites must include the mandatory information such as the name, address, city, state, and country details.

7. In the Aruba Central UI, click **Browse** and add the file from your local directory.
8. Click **Upload**. The sites from the CSV file are added to the site table.

Assigning a Device to a Site

Sites are used to group devices by a physical location. You can assign devices to a site to group them and monitor based on the site name.

To assign devices to a site, complete the following steps:

1. In the **Aruba Central** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
   By default, the **Network Structure** tab is displayed.
3. Click the **Sites** tile.
   The **Manage Sites** page is displayed.
4. Select **Unassigned**. The list of devices that are not assigned to any site is displayed.
5. Select device(s) from the list of devices. To select multiple devices use shift+click or ctrl+click.

NOTE

> It is recommended not to add more than 20 devices at a time for seamless operation.

6. Drag and drop the devices to the site on the left. A pop-up window opens and prompts you to confirm the site assignment.
7. Click **Yes**.

Converting Existing Labels to Sites

Labels are tags attached to devices provisioned in a network. Labels determine the ownership, departments, and functions of the devices. You can covert these labels to sites for creating a logical set of devices.

To convert existing labels to sites, complete the following steps:

1. In the **Aruba Central** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.
   By default, the **Network Structure** tab is displayed.
3. Click the **Sites** tile.
   The **Manage Sites** page is displayed.
4. Click **Convert Labels to Sites**. The **Confirm Conversion** pop-up window opens.
5. To download a CSV file with the list of labels configured in your setup, click **Download file with existing labels**. A CSV file with a list of all the labels in your setup is downloaded to your local directory.
6. Enter address, city, state, country, and ZIP code details for the labels that you want to convert to sites.

NOTE

> In the CSV file, you must enter the following details: address, city, state, and country.

7. Save the CSV file.

- If the conversion process fails for some labels, Aruba Central generates and opens an Excel file showing a list of labels that could not be converted to sites. Verify the reason for the errors, update the CSV file, and re-upload the file.
- Aruba Central does not allow conversion of sites to labels. If the existing labels are converted to sites, you cannot revert these sites to labels.
- When the existing labels are converted to sites, Aruba Central retains only the historical data for these labels. Aruba Central displays the historical data for these labels only in reports and on the monitoring dashboard.

Editing a Site

You can edit a site to modify the site details such as site name, street address, city, county, state, or zip or postal code.

To modify a site details, complete the following steps:

1. In the **Aruba Central** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.

   By default, the **Network Structure** tab is displayed.
3. Click the **Sites** tile.

   The **Manage Sites** page is displayed.
4. Select the site to edit and click the ✎ **edit** icon.
5. Modify the site information and click **Update**.

Deleting a Site

If you no longer need a site, you can delete it.

To delete a site, complete the following steps:

1. In the **Aruba Central** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization**.

   By default, the **Network Structure** tab is displayed.
3. Click the **Sites** tile.

   The **Manage Sites** page is displayed.
4. Select the site to be deleted and click the delete 🗑 icon.

   A confirmation window is displayed.

   NOTE

   Deleting a site disassociates all devices that are associated with it. However, your network and devices will continue to operate normally.
5. Click **Yes** to confirm.

   The site is deleted and devices associated with the site are moved to the unassigned devices list.

REFERENCE 14

Home CLI Release Notes PDFs FAQs Support Knowledge Base Glossary Terminology Change

Search

You are here: Home > Aruba Central Overview > Allowlist Features > Example Use Case

Example Use Case

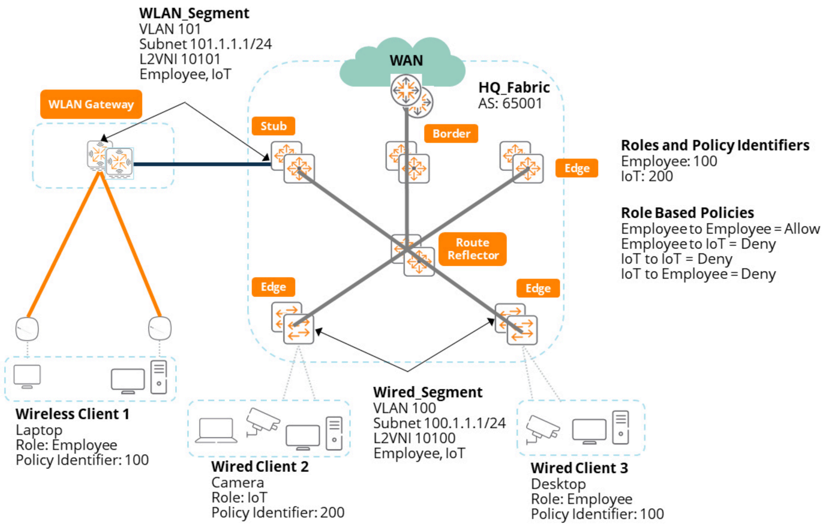
This section describes example use cases for the following deployments:

1. Hybrid Campus-wide Fabric
2. Centralized Multi-site Fabric with Aruba SD-Branch
3. Centralized Multi-site Fabric with Third-Party SD-WAN

Hybrid Campus-wide Fabric

This section describes an example use case for the Hybrid Campus-wide Fabric deployment using Aruba Central.

Figure 1 *Hybrid Campus-wide Fabric Use Case*



In the use case, the goal is to enable role-based micro-segmentation across all wired and wireless clients in an enterprise campus. Roles and role-based policies are orchestrated centrally from the **Client Roles** page on Aruba Central. These policies are enforced on the edge VTEPs in a distributed EVPN fabric for wired clients and on the WLAN gateways for wireless clients. The VXLAN-EVPN fabric is provisioned on the AOS-CX switches using the Fabric Provisioning Wizard on Aruba Central.

As depicted in the above diagram, wired and wireless clients that are assigned the employee role are allowed to communicate with other clients with the Employee role, but not to the clients with the IoT role. Conversely, clients with the IoT role are denied access to clients of both the IoT and employee role.

Step 1: Creating the Role and Role-based Policy

The roles and role-based policies are defined in the **Client Roles** page on Aruba Central. In the **Client Roles** page, the Employee role is created with a policy Identifier 100 and the IoT role is created with a Policy Identifier of 200.

Policies for these roles are defined next. The permission for the Employee role is assigned to allow source to destination. This allows communication between the clients with the Employee role. By default, all other role-based communication is denied.

After the permissions are assigned, this role and policy definition is configured on all gateways and switches on the network.

For more information about how to create role and role-based policy using Aruba Central, refer to Global Client Roles.

Step 2: Creating the Overlay Fabric

The next step is to provision an EVPN-VXLAN fabric on the AOS-CX switches to enable propagation of roles across the network and enforce role-based policies for wired clients. In the **Create a New Fabric** page, a new fabric with the name HQ_Fabric is created with BGP AS 65001, which is auto-populated by Aruba Central. After the fabric is created, the configurations for the EVPN-VXLAN fabric and static VXLAN tunnels are pushed to the AOS-CX devices.

For more information about how to create fabric using Aruba Central, refer to Distributed Overlay Fabric and Overlay Segments.

Step 3: Creating the Wired and Wireless Segment

The Segment Creation wizard is used to create a wired segment and apply the segment to all the Edge VTEPs in a fabric. A segment is created with the name Wired_Segment, VLAN ID 100, and Default Gateway IP of 100.1.1.1/24. The L2VNI of 10100 is auto-assigned to the segment by Aruba Central. The Employee and IoT role is assigned to the segment and applied to all the wired Edge VTEPs in the fabric.

Similarly, a wireless segment is created and applied to the Stub VTEPs that connect to the WLAN gateways in the network. This segment has name Wireless_Segment, VLAN ID 101 and Default Gateway IP of 101.1.1.1/24. The Employee and IoT role is also assigned to the segment and applied to all the Stub VTEPs in the fabric.

For more information about how to create wired and wireless segment using Aruba Central, refer to Distributed Overlay Fabric and Overlay Segments.

Step 4: Creating Static VXLAN Tunnel on the Gateway

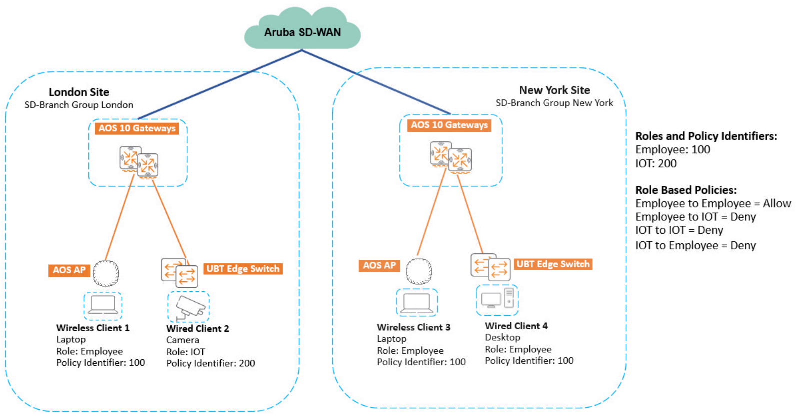
on AOS 10 Gateways.

Upon successful configuration, role-based policies are enforced across all clients in the network. In the example above, Wireless Client 1 which is authenticated with the role Employee communicates with the Wired Client 3 with role Employee but is denied communication with the Wired Client 2 with role IoT. Similarly, the Wired Client 2 cannot communicate with either Wireless Client 1 or Wired Client 3.

Centralized Multi-site Fabric with Aruba SD-Branch

This section describes an example use case for the Centralized Multi-site Fabric with Aruba SD-Branch deployment using Aruba Central.

Figure 2 *Centralized Multi-site Fabric with Aruba SD-Branch Use case*



The SD-Branch group London maps to the London site and the SD-Branch group New York maps to the New York site. The goal is to enable role-based micro-segmentation across multiple geographic sites connected over an Aruba SD-WAN fabric. Roles and role-based policies are centrally in the **Client Roles** page on Aruba Central. The AOS 10 Gateway is the WLAN gateway for the wireless clients and user-based tunnel Gateway for the wired clients within the site. The role-based policies are enforced on the AOS 10 Gateways for all the clients within the site. Role propagation and role-based policy enforcement is selectively enabled per groups.

As depicted in the above diagram, wired and wireless clients that are assigned the Employee role is allowed to communicate with other clients with the Employee role, but not to the clients with the IoT role. Conversely, clients with the IoT role are denied access to clients of both the IoT and Employee role.

Step 1: Creating Role and Role-based Policy

The roles and role-based policies are defined on the **Client Roles** page on Aruba Central. In the **Client Roles** page, the Employee role is created with a Policy Identifier 100 and the IoT role is created with a Policy Identifier of 200.

Policies for these roles are defined. The permission for the Employee role is assigned to allow source to destination. This allows communication only between the clients with the Employee role. By default, all other role-based communication to the

After the permissions are assigned, the same role and policy definition is configured on all gateways and switches on the network.

For more information about how to create role and role-based policy using Aruba Central, refer to Global Client Roles.

Step 2: Selective Enablement of Groups

The next step is to selectively enable the groups that maps to the respective sites. In the **Client Roles** page, select **No** for **Use a switch fabric for a role propagation?** option, and select the **Branch** option. The respective groups are configured to enable role propagation and role-based policy enforcement for those sites.

For more information about how to selectively enable groups for multi-site using Aruba Central, refer to Selective Enablement of Groups.

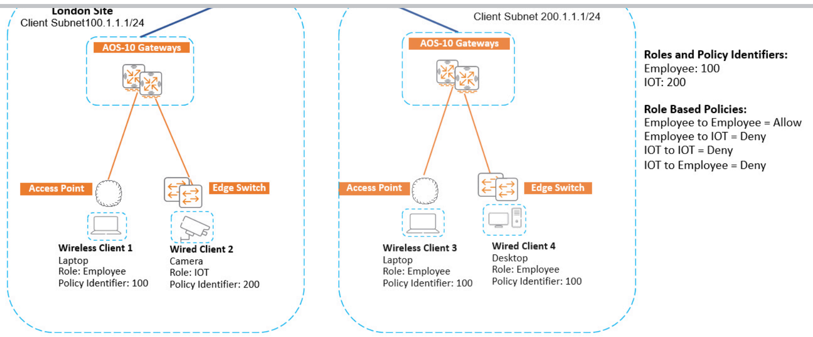
After successfully applying the configuration, role-based policies are enforced on all clients in the network.

In the above example:

- Wireless Client 1 in the London site, which is authenticated with the role Employee communicates with Wired Client 3 with the role Employee in the New York site, but is denied communication with Wired Client 2 with the role IoT, although it is in the same site and group.
- Similarly, Wired Client 2 cannot communicate with either Wireless Client 1 or Wired Client 3.

Centralized Multi-site Fabric with Third-Party SD-WAN

This section describes an example use case for the Centralized Multi-site Fabric with Third-Party SD-WAN deployment using Aruba Central.



In the use case, the client subnet 100.1.1.1/24 maps to clients in the London site and the client subnet 200.1.1.1/24 maps to clients in the New York site. The goal is to enable role-based micro-segmentation across multiple geographic sites connected over a Third-Party SD-WAN fabric. Roles and role-based policies are centrally in the **Client Roles**page on Aruba Central. The third-party gateway is the WLAN gateway for the wireless clients and user-based tunnel Gateway for the wired clients within the site. The role-based policies are enforced on the Third-Party Gateways for all the clients within the site. Role propagation and role-based policy enforcement is selectively enabled per subnets.

As depicted in the above diagram, wired and wireless clients that are assigned the Employee role is allowed to communicate with other clients with the Employee role, but not to the clients with the IoT role. Conversely, clients with the IoT role are denied access to clients of both the IoT and Employee role.

Step 1: Creating Role and Role-based Policy

The roles and role-based policies are defined on the **Client Roles** page on Aruba Central. In the **Client Roles** page, the Employee role is created with a Policy Identifier 100 and the IoT role is created with a Policy Identifier of 200.

Policies for these roles are defined. The permission for the Employee role is assigned to allow source to destination. This allows communication between the clients with the Employee role. By default, all other role-based communication is denied.

After the permissions are assigned, the same role and policy definition is configured on all gateways and switches on the network.

For more information about how to create role and role-based policy using Aruba Central, refer to Global Client Roles.

Step 2: Selective Enablement of Subnets

The next step is to selectively enable the subnets that maps to the clients in the respective sites. In the **Client Roles** page, select **No** for **Use a switch fabric for a role propagation?** option, and select the **Mobility** option. . The respective client subnets are configured to enable role propagation and role-based policy enforcement for those sites.

For more information about how to selectively enable subnets for multi-site using Aruba Central, refer to Selective Enablement of Subnets.

After successfully applying the configuration, role-based policies are enforced on all clients in the network.

In the above example:

- Wireless Client 1 in the London site, which is authenticated with the role Employee communicates with Wired Client 3 with the role Employee in the New York site, but is denied communication with Wired Client 2 with the role IoT, although it is in the same site and subnet.
- Similarly, Wired Client 2 cannot communicate with either Wireless Client 1 or Wired Client 3.

REFERENCE 15

TECHNICAL WHITEPAPER

VXLAN INTEROPERABILITY

ARUBAOS-SWITCH CONFIGURATION GUIDE

aruba
a Hewlett Packard Enterprise company

[Reference 15]

Contents

[Reference 15]

INTRODUCTION

Virtual eXtensible LAN (VXLAN) is a MAC-in-UDP technology that provides Layer 2 connectivity between distant network sites across an IP network. VXLAN is typically used in data centers for multitenant services.

VXLAN provides the following benefits:

- Support for more virtual switched domains than VLANs. Each VXLAN is uniquely identified by a 24-bit VXLAN ID. The total number of VXLANs can reach 16777216 (2^{24}). This specification makes VXLAN a better choice than 802.1Q VLAN to isolate traffic for virtual machines (VMs).
- Easy deployment and maintenance. VXLAN requires deployment only on the edge devices of the transport network. Devices in the transport network perform Layer 3 forwarding.

The VXLAN tunnel endpoints (VTEP) performs Layer 2 or Layer 3 forwarding for VXLANs depending on your configuration:

- In Layer 3 forwarding mode, the VTEP uses the ARP table to forward traffic for VXLANs. Use Layer 3 forwarding mode if you want to use the VTEP as a VXLAN IP gateway.
- In Layer 2 forwarding mode, the VTEP uses the MAC address table to forward traffic for VXLANs.

This whitepaper describes the Layer 2 forwarding processes. It describes how to configure a VXLAN tunnel between an HPE FlexFabric 12900 and an Aruba 3810M, supporting VXLAN. Please note that only FC, FE, and FX cards on the 12900 support VXLAN.

Note: The configuration examples in this document should be limited to very small deployments, considering the large amount of configuration required to configure the static VXLAN tunnels.

LOGICAL NETWORK DIAGRAM

As shown in the figure below, the end devices are Aruba 2540 and 2930M switches. The VTEPs are the VXLAN tunnel endpoints. For this document, we use the HPE 12900 and the Aruba 3810M Switch Series as VTEPs.

A VTEP uses Virtual Switch Instances (VSIs) and VXLAN tunnels to provide VXLAN services.

- Virtual Switch Instance (VSI) – A VSI is a virtual Layer 2 switched domain. Each VSI provides switching services only for one VXLAN. VSIs learn MAC addresses and forward frames independently of one another. VMs in different sites have Layer 2 connectivity if they are in the same VXLAN.
- VXLAN tunnel – VXLAN tunnels are logical point-to-point tunnels between VTEPs over the transport network. Each VXLAN tunnel can trunk multiple VSLANs. VTEPs encapsulate VXLAN traffic in the VXLAN, outer UDP, and outer IP headers. The devices in the transport network forward VXLAN traffic only based on the outer IP header.

VTEPs encapsulate VXLAN traffic in the VXLAN, outer UDP and outer IP headers. The devices in the transport network forward VXLAN traffic only based on the outer IP header.

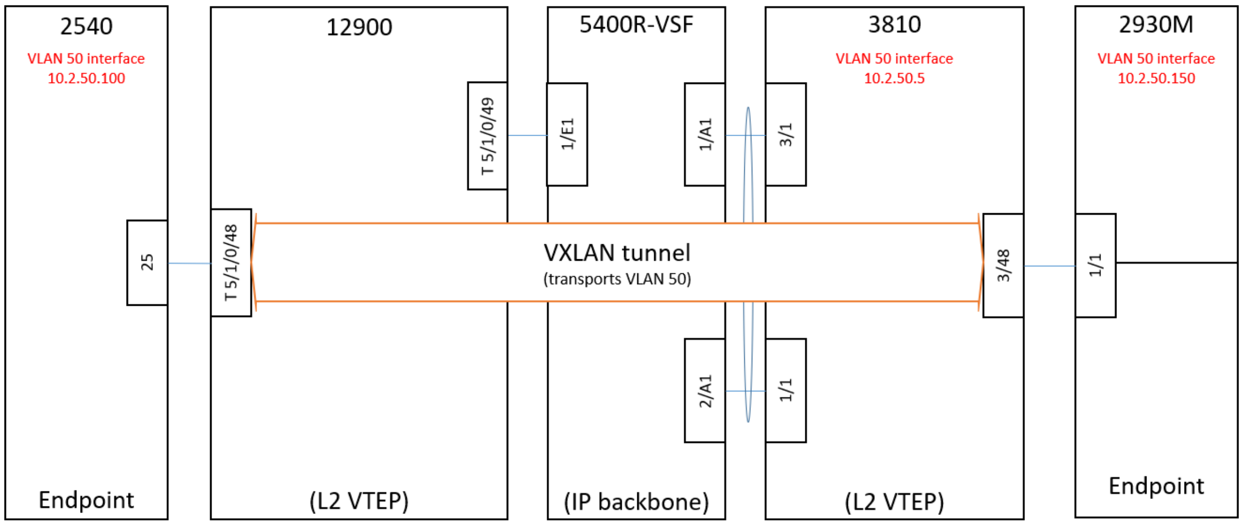


Figure 1: Logical Network Diagram

WORKING MECHANISMS

The VTEP uses the following process to forward an inter-site frame:

- Assigns the frame to its matching VXLAN if the frame is sent between sites.
- Performs MAC learning on the VXLANs VSI.
- Forwards the frame.

VXLAN tunnel establishment and assignment

To provide Layer 2 connectivity for a VXLAN between two sites, you must create a VXLAN tunnel between the sites and assign the tunnel to the VXLAN.

Traffic from the local site to a remote site

The VTEP uses and Ethernet service instance to match a list of VLANs on a site-facing interface. The VTEP assigns customer traffic from the VLANs to a VXLAN by mapping the Ethernet service instance to a VSI.

Traffic from a remote site to the local site

When a frame arrives at a VXLAN tunnel, the VTEP uses the VXLAN ID in the frame to identify its VXLAN.

MAC Learning

The VTEP performs source MAC learning on the VSI as a Layer 2 switch.

- For traffic from the local site to the remote site, the VTEP learns the source MAC address before VXLAN encapsulation.
- For traffic from the remote site to the local site, the VTEP learns the source MAC address after removing the VXLAN header.

Traffic Forwarding

The VTEP performs Layer 2 or Layer 3 forwarding for VXLANs depending on your configuration:

- In Layer 3 forwarding mode, the VTEP uses the ARP table to forward traffic for VXLANs. Use Layer 3 forwarding mode if you want to use the VTEP as a VXLAN IP gateway.

[Reference 15]

- In Layer 2 forwarding mode, the VTEP uses the MAC address table to forward traffic for VXLANs.

HARDWARE AND SOFTWARE REQUIREMENTS

For this document, the following hardware and software versions were used in order to implement this specific VXLAN solution:

- Aruba 3810M Switch Series – KB.16.08.0001
- HPE 12900 and FX Module (JH359A) – version 7.1.070, Release 2712

CONFIGURATION

The following steps are to configure VXLAN on the HPE FlexFabric 12900 and on the Aruba 3810M. The prerequisites are to configure IP addresses and unicast routing settings on all transport switches:

- Assign IP addresses to the interfaces
- Configure OSPF on all transport network switches
- Configure OSPF to advertise routes

HPE FlexFabric 12900 Configuration

Create a VLAN for the endpoint devices

```
vlan 50
interface Vlan-interface50
 ip address 10.2.50.10 255.255.255.0
```

Enable L2VPN

```
system-view
l2vpn enable
```

Enable Layer 2 Fowarding

```
undo vxlan ip-forwarding
```

Create the VSI vni200 and VXLAN 200

```
vsi vni200
 vxlan 200
 quit
 quit
```

Assign an IP address to Loopback 0. The IP address will be used as the source IP address of the VXLAN tunnels to Switch B and Switch C.

```
interface LoopBack0
 ip address 5.8.1.10 255.255.255.255
 ospf 1 area 0.0.0.0
```

Create a VXLAN tunnel to the 3810M. The tunnel interface name is Tunnel 13

```
interface Tunnel13 mode vxlan
 source 5.8.1.10
 destination 5.8.1.2
 quit
```

Assign Tunnel 13 to VXLAN 200.

```
vsi vni200
 vxlan 200
  tunnel 13
  quit
 quit
```

On the uplink to the 3810M create Ethernet service instance 2.

```
interface Ten-GigabitEthernet5/1/0/48
 port link-mode bridge
 port access vlan 50
 service-instance 2
  encapsulation untagged
```

Map Ethernet service instance 2 to the VSI vni200.

```
interface Ten-GigabitEthernet4/0/1
service-instance 2
xconnect vsi vni200
quit
quit
```

Configure the uplink to the endpoint device

```
interface Ten-GigabitEthernet5/1/0/49
 port link-mode route
 ip address 10.220.0.2 255.255.255.252
 ospf network-type p2p
 ospf 1 area 0.0.0.0
```

Aruba 3810 configuration

Enable VXLAN

```
vxlan enable
```

Create Virtual Network and associate Virtual Network ID to VLAN

```
virtual-network 200 50 "vni200"
```

Create VXLAN tunnel between the two switches

```
interface tunnel 13
   tunnel name "VXLAN_Tunnel02"
   tunnel mode vxlan
   tunnel source 5.8.1.2
   tunnel destination 5.8.1.10
   exit
```

Map Overlay-VLAN (VLAN 50) to Tunnel 13

```
vxlan tunnel 13 overlay-vlan 50
```

[Reference 15]

VERIFICATION

As mentioned in the introduction, the VXLAN tunnel endpoints are HPE 5700 and Aruba 2920 switches. Below are the details of the endpoints.

Table 1: VXLAN tunnel endpoints

Model	IP Address	MAC Address
Aruba 2540	10.2.50.100	98:f2:b3:c0:a5:00
Aruba 2930M	10.2.50.150	F4:03:43:de:27:47

The commands to determine the information in Table 1 above are:

```
2540Switch(config)# show arp

 IP ARP table

  IP Address       MAC Address        Type    Port
  ---------------  -----------------  ------- ----
  10.2.50.150      f40343-de2747      dynamic

2930MSwitch(config)# show arp

 IP ARP table

  IP Address       MAC Address        Type    Port
  ---------------  -----------------  ------- ----
  10.2.50.100      98f2b3-c0a500      dynamic
```

To confirm that the above data is correct, issue the following commands on both endpoints to find out the MAC address for each interface:

```
2930MSwitch(config)# show system

 Status and Counters - General System Information

  System Name          : Aruba-Stack-2930M
  System Contact       :
  System Location      :
  MAC Age Time (sec)   : 300
  Time Zone            : 0
  Daylight Time Rule   : None

  Software revision    : WC.16.08.0001
  Base MAC Addr        : f40343-de2747

 Member :1

  ROM Version          : WC.17.02.0006
  Up Time              : 2 days
  CPU Util (%)         : 0
  MAC Addr             : f40343-de2740
  Serial Number        : SG7ZJQP03Y
  Memory    - Total    : 340,857,344
              Free     : 180,406,648
2540Switch(config)# show system

 Status and Counters - General System Information

  System Name         : Aruba-2540-24G-PoEP-4SFPP
  System Contact      :
  System Location     :

  MAC Age Time (sec)  : 300

  Time Zone           : 0
  Daylight Time Rule  : None

  Software revision   : YC.16.08.0002        Base MAC Addr      : 98f2b3-c0a500
  ROM Version         : YC.16.01.0002        Serial Number      : CN77JYK05S

  Up Time             : 2 days               Memory    - Total  : 360,047,104
  CPU Util (%)        : 2                              Free     : 258,874,500

  IP Mgmt   - Pkts Rx : 8284                 Packet    - Total  : 6600
              Pkts Tx : 8272                 Buffers     Free   : 4859
                                                         Lowest : 4853
                                                         Missed : 0
```

To verify the correct neighbor information, issue the following LLDP commands:

```
<12904-2>disp lldp neighbor-information list
Chassis ID : * -- -- Nearest nontpmr bridge neighbor
             # -- -- Nearest customer bridge neighbor
             Default -- -- Nearest bridge neighbor
Local Interface Chassis ID      Port ID                    System Name
XGE5/1/0/3      943f-c206-dfbb  Ten-GigabitEthernet1/0/18  5940-4
XGE5/1/0/4      d894-0322-1e30  Ten-GigabitEthernet1/1/18  5940-3
XGE5/1/0/7      d894-03f8-8baa  Ten-GigabitEthernet1/2/18  5940-6
XGE5/1/0/48     98f2-b3c0-a500  25                         Aruba-2540-24G-PoEP-4SFPP
XGE5/1/0/49     5820-b1b2-9b3f  129                        M1st-Core
3810(config)# show lldp info remote-device

 LLDP Remote Devices Information

  LocalPort | ChassisId          PortId             PortDescr SysName
  --------- + ------------------ ------------------ --------- ------------------
  1/1       | 5820b1-b29b3f      1                  1/A1      M1st-Core
  1/23      | 40e3d6-c42964      40 e3 d6 c4 29 64  eth0      40:e3:d6:c4:29:64
  1/24      | d4c9ef-f81b0d      d4 c9 ef f8 1b 0d
  3/1       | 5820b1-b29b3f      193                2/A1      M1st-Core
  3/24      | 10604b-471e6a      10 60 4b 47 1e 6a
  3/24      | 0.0.0.0            2c 41 38 7f a8 d5
  3/48      | f40343-de2747      1                  1/1       Aruba-Stack-2930M
```

Now traffic can be passed between the two endpoints:

```
2540Switch(config)# ping 10.2.50.150
10.2.50.150 is alive, time = 3 ms


2930MSwitch(config)# ping 10.2.50.100
10.2.50.100 is alive, time = 2 ms
```

Besides pinging the two endpoint devices, in order to verify the correct functionality, the status of the tunnels and MAC learning, issue the following commands:

On the 12900

```
<12904-2>display interface tunnel 13
Tunnel13
Current state: UP
Line protocol state: UP
Description: Tunnel13 Interface
Bandwidth: 64 kbps
Maximum transmission unit: 1464
Internet protocol processing: Disabled
Last clearing of counters: Never
Tunnel source 5.8.1.10, destination 5.8.1.2
Tunnel protocol/transport UDP_VXLAN/IP
```

Verify that the VXLAN tunnels have been assigned:

```
<12904-2>display l2vpn vsi verbose
VSI Name: vni200
  VSI Index               : 0
  VSI State               : Up
  MTU                     : 1500
  Bandwidth               : Unlimited
  Broadcast Restrain      : Unlimited
  Multicast Restrain      : Unlimited
  Unknown Unicast Restrain: Unlimited
  MAC Learning            : Enabled
  MAC Table Limit         : -
  MAC Learning rate       : -
  Drop Unknown            : -
  Flooding                : Enabled
  Statistics              : Disabled
  VXLAN ID                : 200
  Tunnels:
    Tunnel Name          Link ID    State    Type        Flood proxy
    Tunnel13             0x500000d  UP       Manual      Disabled
  ACs:
    AC                               Link ID  State       Type
    XGE5/1/0/48 srv2                 0        Up          Manual
```

Verify that the VTEP has learned the MAC addresses of remote devices:

```
<12904-2>display l2vpn mac-address
MAC Address    State    VSI Name                          Link ID/Name    Aging
98f2-b3c0-a500 Dynamic  vni200                            XGE5/1/0/48     Aging
f403-43de-2747 Dynamic  vni200                            Tunnel13        Aging
--- 2 mac address(es) found  ---
```

On the 3810M

Verify the interface tunnel

```
3810(config)# show interface tunnel

 Tunnel Configuration :

  Tunnel                   : 251659491
  Tunnel Name              : VXLAN_Tunnel02
  Tunnel Status            : Enabled
  Source Address           : 5.8.1.2
  Destination Address      : 5.8.1.10
  Mode                     : VXLAN Tunnel
  TOS                      : -1
  TTL                      : 64
  IPv6                     : n/a
  MTU                      : 1450


 Current Tunnel Status :

  Tunnel State                  : Up
  Destination Address Route : 5.8.1.10/32
  Next Hop IP                   : 10.30.1.254
  Next Hop Interface            : vlan-30
  Next Hop IP Link Status       : Up
  Source Address                : 5.8.1.2
```

Verify that the VXLAN tunnels have been assigned

```
3810(config)# show virtual-network
  Max. Supported Virtual Networks    : 64
  Virtual Networks Configured        : 1

  VN-ID VN-Name                         VLAN-ID VLAN-Name
  ----- ------------------------------- ------- --------------------------------
  200   vni200                          50      VLAN50
```

APPENDIX A – SWITCH CONFIGURATIONS

3810 configuration

```
; hpStack_KB Configuration Editor; Created on release #KB.16.08.0001
; Ver #0c:01.7c.59.f4.7b.ff.ff.fc.ff.ff.3f.ef:
stacking
   member 1 type "JL074A" mac-address 70106f-8fa780
   member 1 priority 255
   member 2 type "JL076A" mac-address 1c98ec-9e0f80
   member 2 priority 200
   member 3 type "JL076A" mac-address 1c98ec-9e4d00
   member 3 priority 150
   member 3 flexible-module A type JL083A
   exit
hostname "3810"
no rest-interface
vxlan enable
vxlan tunnel 13 overlay-vlan 50
trunk 1/1,3/1 trk1 lacp
max-vlans 4000
ip routing
interface loopback 0
   ip address 5.8.1.2
   ip ospf 5.8.1.2 area backbone
   exit
interface tunnel 13
   tunnel name "VXLAN_Tunnel02"
   tunnel mode vxlan
   tunnel source 5.8.1.2
   tunnel destination 5.8.1.10
   exit
snmp-server community "public" operator unrestricted
snmp-server community "private"
oobm
   ip address dhcp-bootp
   ipv6 enable
   ipv6 address dhcp full
   member 1
      ip address dhcp-bootp
      ipv6 enable
      ipv6 address dhcp full
      exit
   member 2
```

[Reference 15]

```
      ip address dhcp-bootp
      ipv6 enable
      ipv6 address dhcp full
      exit
   member 3
      ip address dhcp-bootp
      ipv6 enable
      ipv6 address dhcp full
      exit
   exit
router ospf
   area backbone
   enable
   exit
vlan 1
   name "DEFAULT_VLAN"
   no untagged 1/D4,2/D4,Trk1-Trk2
   untagged 1/D2-1/D3,1/D6-1/D7,1/F1-1/F24,2/D2-2/D3,2/D6-2/D7
   ip address dhcp-bootp
   exit
vlan 10
   name "VLAN10"
   untagged 1/11
   ip address 10.5.8.4 255.255.255.0
   ip ospf 10.5.8.4 area backbone
   jumbo
   exit
vlan 20
   name "VLAN20"
   no ip address
   exit
vlan 30
   name "VLAN30"
   untagged Trk1
   ip address 10.30.1.4 255.255.255.0
   ip ospf 10.30.1.4 area backbone
   exit
vlan 40
   name "VLAN40"
   ip address 10.2.40.5 255.255.255.0
   ip ospf 10.2.40.5 area backbone
   exit
vlan 50
   name "VLAN50"
   untagged 3/48
   ip address 10.2.50.5 255.255.255.0
   exit
spanning-tree Trk1 priority 4
virtual-network 200 50 "vni200"
password manager
```

12900 Switch Configuration

```
#
 version 7.1.070, Release 2712
#
mdc Admin id 1
#
mdc Production-MDC id 2
 mdc start
#
 sysname 12900
#
 telnet server enable
#
 undo vxlan ip-forwarding
#
ospf 1
 non-stop-routing
 area 0.0.0.0
  network 1.220.0.2 0.0.0.0
  network 5.8.1.10 0.0.0.0
  network 10.2.10.0 0.0.0.255
  network 10.220.0.0 0.0.0.3
#
 lldp global enable
#
 mvrp global enable
#
 reserve-vlan-interface 3000 to 3100
 reserve-vlan-interface 200 global
#
 system-working-mode standard
 password-recovery enable
 lpu-type f-series
#
vlan 1
#
vlan 50
#
vlan 129
#
```

```
 stp global enable
#
 l2vpn enable
#
vsi vni200
 vxlan 200
  tunnel 13
#
interface NULL0
#
#
interface LoopBack0
 ip address 5.8.1.10 255.255.255.255
 ospf 1 area 0.0.0.0
#
interface Vlan-interface1
 mtu 9008
#
interface Vlan-interface50
 ip address 10.2.50.10 255.255.255.0
#
interface FortyGigE5/0/1
 port link-mode route
#
interface FortyGigE5/0/13
#
# ... other interfaces ...
#
interface M-GigabitEthernet0/0/0
 ip address 10.10.10.44 255.255.255.0
#
interface Ten-GigabitEthernet5/1/0/48
 port link-mode bridge
 port access vlan 50
 #
 service-instance 2
  encapsulation untagged
  xconnect vsi vni200
#
interface Ten-GigabitEthernet5/1/0/49
 port link-mode route
 ip address 10.220.0.2 255.255.255.252
 ospf network-type p2p
 ospf 1 area 0.0.0.0
#
```

[Reference 15]

```
interface Ten-GigabitEthernet4/0/3
 port link-mode bridge
#
interface Ten-GigabitEthernet4/0/4
 port link-mode bridge
#
interface Ten-GigabitEthernet4/0/5
 port link-mode bridge
#
interface Ten-GigabitEthernet4/0/6
 port link-mode bridge
#
interface Ten-GigabitEthernet4/0/7
 port link-mode bridge
#
interface Ten-GigabitEthernet4/0/8
 port link-mode bridge
#
# ... other interfaces ...
#
#
interface Tunnel13 mode vxlan
 source 5.8.1.10
 destination 5.8.1.2
#
interface Blade-Aggregation1
#
 scheduler logfile size 16
#
line class aux
 user-role network-admin
#
line class vty
 user-role network-operator
#
line aux 0 1
 user-role network-admin
#
#
line vty 0 15
 authentication-mode scheme
 user-role network-operator
#
line vty 16 63
 user-role network-operator
```

[Reference 15]

```
#
 ip route-static 0.0.0.0 0 10.10.10.254
#
 snmp-agent
 snmp-agent local-engineid 800063A28080F62E82C30700000001
 snmp-agent community write private
 snmp-agent community read public
 snmp-agent sys-info version all
 snmp-agent target-host trap address udp-domain 10.10.10.10 params
securityname public v2c
 snmp-agent target-host trap address udp-domain 10.3.10.220 params
securityname public v2c
#
acl number 2000
#
acl number 3000
#
acl number 4000
domain system
#
 domain default enable system
#
role name level-0
 description Predefined level-0 role
#
role name level-1
 description Predefined level-1 role
#
role name level-2
 description Predefined level-2 role
#
role name level-3
 description Predefined level-3 role
#
role name level-4
 description Predefined level-4 role
#
role name level-5
 description Predefined level-5 role
#
role name level-6
 description Predefined level-6 role
#
role name level-7
 description Predefined level-7 role
```

[Reference 15]

```
#
role name level-8
 description Predefined level-8 role
#
role name level-9
 description Predefined level-9 role
#
role name level-10
 description Predefined level-10 role
#
role name level-11
 description Predefined level-11 role
#
role name level-12
 description Predefined level-12 role
#
role name level-13
 description Predefined level-13 role
#
role name level-14
 description Predefined level-14 role
#
user-group system
#
local-user admin class manage
 password hash
$h$6$ucKzWby6Pa3zRhCP$uCDJbw5pvcGP9gIFXP0I4++QDxc9sXvPK8WrwhpwbgK976oHF5r06yL
mvdzUcJwOxz6PxwgKu/MRapealGtgsA==
 service-type telnet
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
return
```

For more information

http://www.arubanetworks.com/

aruba
a Hewlett Packard
Enterprise company
www.arubanetworks.com

3333 Scott Blvd | Santa Clara, CA 95054
1.866.55.ARUBA | T: 1.408.227.4500 | FAX: 1.408.227.4550 | info@arubanetworks.com

[Reference 15]